VEILIGHEIDSZORG
EN
DIGITALISERING VAN DREIGINGEN

Masterthesis
Tim Puts - 0623628
Opleiding Bestuurskunde
Faculteit der Managementwetenschappen
Radboud Universiteit Nijmegen
Augustus 2019
Begeleidend docent dhr. prof. dr. T. Brandsen
Word count 30 594

Pagina intentioneel leeg gelaten

Dank, aan eenieder die op welke wijze dan ook
betrokken is geweest bij de totstandkoming van deze thesis

Peia
Projectgroep ‘Digitale ontwrichting’, WRR
Familie en vrienden

INHOUD

HOOFDSTUK EEN
INLEIDING

Koningsdag. In heel Nederland zijn festiviteiten, vlooienmarkten en optredens aan de gang. Mede vanwege het mooie weer zijn er enorme mensenmassa's op de been; ze bestaan uit dagjesmensen, locals en toeristen. Om zeven uur 's avonds beginnen de eerste problemen; een storing in de pinsystemen zorgt ervoor dat bij de meeste festivalterreinen, buitenbars, foodtrucks en pop-up restaurants in heel het land niet meer met betaalkaarten betaald kan worden. Cash betalingen waren sowieso op veel plaatsen al niet mogelijk[1], dus het betalingsverkeer ligt stil. Ook pinautomaten, betaalautomaten en de laadpalen van het openbaar vervoer zijn niet te gebruiken[2]. De verstoringen blijken zich echter niet tot dergelijke systemen te beperken. Ook communicatie- en informatiesystemen weigeren dienst, waardoor belangrijke delen van het openbaar vervoer rondom Utrecht Centraal, Amsterdam Centraal en Schiphol plat komen te liggen. Logischerwijs vermoeden veel mensen, voor festiviteiten naar de grote steden uitgeweken, dat ze moeilijkheden gaan ondervinden om nog thuis te komen. Veel van hen besluiten nu vast naar de treinstations te gaan om nog kans te hebben thuis te komen, en komen dus voor teleurstelling te staan[3]. Rondom de stations ontstaan vervelende situaties door mensen die niet goed weten hoe ze thuis gaan komen.

Op de weg ontstaan ook problemen doordat verkeerslichten, matrixborden en informatiesystemen boven de weg ontregeld zijn. Ongelukken blijven uit omdat men rekening met elkaar houdt, maar van goede doorstroming van het verkeer is geen sprake[4], mede vanwege de grote hoeveelheid auto's op de weg: mensen die met de auto familie en vrienden ophalen omdat het openbaar vervoer niet te gebruiken is. De politie wordt ingezet om de openbare orde te handhaven, bij het NCSC wordt een crisisteam samengeroepen om de gevolgen voor de Rijksoverheid en vitale sectoren te monitoren. Al gauw wordt duidelijk dat de verstoringen het gevolg zijn van een grote *ransomware*-aanval, in combinatie met *DDoS*-aanvallen op verschillende doelwitten. De Minister van Defensie houdt zich aan het door Nederland ingezette attributiebeleid[5]: ze laat op een ingelaste persconferentie weten dat er sterke vermoedens bestaan dat de Russische militaire inlichtingendienst *'GROe'* achter de aanvallen zit[6], maar dat ook een hackersgroep met anti-koningshuissentimenten nog niet kan worden uitgesloten. Wat wel vaststaat, is dat de aanvallers gebruik hebben gemaakt van kwetsbaarheden waarvoor al eerder gewaarschuwd is, maar nog geen oplossing is gevonden: door 'slimme' apparaten in te lijven in botnets en daarmee netwerken te infecteren en systemen plat te leggen[7]. Dit betekent dat naast de eerder genoemde systemen en netwerken ook apparaten van ondernemers en mensen thuis geïnfecteerd kunnen zijn.

Om de aanval de baas te kunnen wordt in samenwerking tussen krijgsmacht, politie, internet serviceproviders en een aantal grote consultancybedrijven met expertise een '*response centre*' ingericht, waar zo'n 600 teamleden op nieuw aangeschafte computers en laptops en

[1] gebaseerd op https://financeinnovation.nl/betalen-op-festivals-cash-verlaat-de-wei/
[2] gebaseerd op https://nos.nl/artikel/2241222-grote-pinstoring-maestro-maar-problemen-lijken-verholpen.html
[3] gebaseerd op https://www.nrc.nl/nieuws/2018/10/04/wat-als-het-internet-uitvalt-a2180425
[4] gebaseerd op https://rijkswaterstaatverkeersinformatie.nl/Nieuws/article/VID.2008.153.02
[5] zie https://www.security.nl/posting/609412/Minister%3A+attributie+maakt+Nederland+minder+aantrekkelijk+doelwit
[6] gebaseerd op https://www.nrc.nl/nieuws/2018/10/04/britse-regering-leger-rusland-zit-achter-cyberaanvallen-a2171680
[7] gebaseerd op https://www.tubantia.nl/tech/ut-professor-slimme-apparaten-maken-ons-kwetsbaar-voor-megacyberaanval~a49ab321

geïmproviseerde WiFi-hotspots aan de slag gaan met het opruimen van het digitale slagveld door het runnen van backups en het mitigeren van de infecties[8]. Omdat ook veel apparaten van burgers en kleinere bedrijven mogelijk met de ransomware geïnfecteerd kunnen zijn, laat de overheid instructies uitgaan voor het opschonen en beschermen van geïnfecteerde apparaten. Het advies aan mensen die er zelf niet uitkomen is om contact op te nemen met securitybedrijven, handige IT'ers in de directe omgeving, en internet serviceproviders.

De grootste verstoringen zijn na anderhalve dag voorbij. De meeste mensen hebben hun weg naar huis inmiddels gevonden, en de meeste apparaten en netwerken zijn weer operatief. De media en bedrijven proberen de totale schade te berekenen. Eerste schattingen: tussen de 250 en 300 miljoen euro[9]. De zoektocht naar de daders is nog bezig, de Russen ontkennen in alle toonaarden.

1.1 Aanleiding

Hoewel bovenstaand scenario als geheel fictief is, zijn delen ervan gebaseerd op daadwerkelijk gebeurde incidenten. Dreigingen die zich via digitale kanalen materialiseren kunnen zorgen voor (grootschalige) verstoringen in het digitale én fysieke domein. Wat het scenario onder meer illustreert, is dat de opkomst en steeds grotere impact van dergelijke dreigingen het leveren van veiligheid als publieke dienst door de overheid onder druk zet. Dit leidt onderzoekers ertoe zich af te vragen of de klassieke veiligheidssystemen zoals politie en krijgsmacht, nog wel op de juiste manier zijn georganiseerd (Brenner, 2014; Chang et al., 2018). Immers, cyber zorgt er onder meer voor dat de onderscheiden waarop bestaande instituties zijn gebaseerd, vervagen: inmiddels kan een veelvoud aan actoren via een veelvoud aan kanalen een veelvoud aan doelwitten raken, middels een veelvoud aan dreigingen. Deze dreigingen zijn bovendien steeds moeilijker te voorkomen, moeilijker te attribueren, moeilijker te classificeren en moeilijker te adresseren.

Digitalisering zorgt niet enkel voor nieuwe kansen en dreigingen, gebruiksgemak en razendsnelle ontwikkelingen, maar ook voor verschuivingen in de verhoudingen tussen maatschappelijke actoren. Overheden en burgers zijn voor allerhande diensten en producten in steeds grotere mate afhankelijk van (grote, buitenlandse) technologiebedrijven op gebieden als (al dan niet vitale) infrastructuur, privacy, communicatiemiddelen en informatiedeling. Ook de veiligheidszorg (de bescherming tegen dreigingen) lijkt niet meer enkel door de overheid als unitaire actor te kunnen worden geleverd. Private partijen zijn steeds vaker een ketenpartner in de veiligheidszorg, en de overheid 'slechts' één van de actoren die veiligheid als publieke dienst bieden (Van Creveld, 1999). Naarmate oorlogsvoering meer digitaal plaatsvindt zijn technologiebedrijven (vanwege hun expertise, marktposities, algoritmen, datasets en budgetten) onmisbaar voor de krijgsmacht[10], en dat is niet oncontroversieel[11]. En naarmate criminaliteit meer digitaal plaatsvindt worden ISPs, private securitybedrijven en dezelfde technologiebedrijven onontbeerlijk in samenwerking met de politionele macht (Lone et al., 2014).

Naast de steeds belangrijkere rol voor private partijen in het leveren van veiligheidszorg, worden ook burgers actief aangespoord hun verantwoordelijkheid te nemen

[8] gebaseerd op https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[9] gebaseerd op https://www.nrc.nl/nieuws/2018/10/04/wat-als-het-internet-uitvalt-a2180425

[10] zie ook https://aiv-advies.nl/download/ec0c2ccc-2946-4100-886a-b72b87df03d0.pdf

[11] zie bijvoorbeeld het rapport van vredesorganisatie PAX, dat de werkzaamheden van bedrijven als Amazon en Microsoft voor het Amerikaanse Pentagon als 'zeer zorgwekkend' classificeert: https://www.paxforpeace.nl/media/files/pax-report-killer-robots-dont-be-evil.pdf

om digitale dreigingen te controleren[12]. Voor hun eigen veiligheid, maar ook voor de veiligheid van de samenleving en de digitale infrastructuur als geheel. 'We zijn zo veilig als de zwakste schakel', is (hoewel niet onomstreden[13]) het idee. De verantwoordelijkheid die bij burgers belegd wordt, lijkt echter in een te kleine mate te worden genomen: basismaatregelen krijgt men maar niet op orde, en hoewel men zichzelf ook als hoofdverantwoordelijke ziet voor de eigen digitale veiligheid thuis is cybersecurity nagenoeg nooit topprioriteit, alle wachtwoorden, updates, afgeplakte camera's en tweestapsverificatie ten spijt. Toch zijn burgers inmiddels een integraal onderdeel van de veiligheidszorg ten aanzien van digitalisering. De politie laat vrijwilligers online patrouilleren, er blijven overheidscampagnes lopen ('*ik blijf het toch zeggen!*'[14]), en maatschappelijke actoren als banken, securitybedrijven en werkgevers blijven mensen op de dreigingen attenderen. De burger *moet* meedoen.

1.2 Probleemstelling

Enerzijds lijkt er op basis van bovenstaande sprake van een ontwikkeling richting breder gedeelde verantwoordelijkheid voor de veiligheidszorg, ten gevolge van digitalisering. In dit geval zou een trend van *decentralisatie* opgemerkt kunnen worden, waarbij overheden met private partners netwerkrelaties aangaan en van burgers verwacht wordt dat zij een actieve rol spelen bij de totstandkoming van veiligheidszorg als publieke dienst. Het scenario waarmee dit hoofdstuk opende illustreert dat ook. Een dergelijke totstandkoming van de veiligheidszorg zou passend zijn bij de hedendaagse stijl van openbaar bestuur, ook wel aangeduid als New Public Governance (Pestoff, 2018; Osborne, 2006). Anderzijds leidt digitalisering tot de internationalisering van dreigingen en maakt het dreigingen (en mogelijke oplossingen) tot een aangelegenheid voor technische specialisten. Om op deze ontwikkelingen in te kunnen spreken, valt een trend van grotere *centralisatie* te verwachten. Immers, enkel centrale overheden zijn opgewassen tegen (internationale) actoren van wie soms niet eens duidelijk is of het gaat om criminelen, kwajongens of een andere staat. Een dergelijke trend zou passen bij het algemene beeld dat heerst ten aanzien van de traditionele veiligheidsapparaten: hiërarchische, top-down organisaties met een command-and-control structuur.

Bovengenoemde trends zijn elkaar tegengestelden. Beiden zouden echter vergaande implicaties kunnen hebben voor de manier waarop dreigingen gecontroleerd gaan worden, de invloed van het openbaar bestuur op de veiligheid van en in staten, en de prijs die voor die veiligheid betaald dient te worden. In het eerste geval (decentralisering) komen belangrijke verantwoordelijkheden (en wellicht ook bevoegdheden) voor de omgang met gepercipieerde dreigingen mogelijk in de handen van private actoren als bedrijven en burgers te liggen. In het tweede geval (centralisering) bestaat de mogelijkheid dat overheidsorganisaties zullen proberen hun invloed in, en controle over, het digitale domein te vergroten om de veiligheid ten aanzien van gepercipieerde digitale dreigingen te garanderen. Hoe dan ook valt te verwachten dat de rol van de overheid ten aanzien van het leveren van veiligheidszorg zal veranderen, onder meer ten gevolge van de digitalisering van dreigingen (Brenner, 2014; Van Creveld, 1999). De overheid is *óf* één van de ketenpartners en medeproducent, *óf* de actor die poogt centraal te sturen.

[12] zie ook https://www.dcypher.nl/sites/default/files/uploads/documents/Rapport%20_Digitale%20Hygiene%20Nederland%20-%20Juni%202018_.pdf

[13] zie ook https://www.schneier.com/blog/archives/2016/10/security_design.html

[14] zie https://www.maakhetzeniettemakkelijk.nl/

Om inzichtelijk te krijgen in welke richting de totstandkoming van de veiligheidszorg ten aanzien van digitalisering beweegt, en wat dit betekent voor de maatschappelijke verhoudingen, worden in deze thesis de onderlinge verhoudingen tussen een viertal cases onder invloed van digitale dreigingen, geanalyseerd: de klassieke systemen voor veiligheidszorg (krijgs- en politionele macht), en bedrijven en burgers als hun mogelijke ketenpartners. De te beantwoorden onderzoeksvraag is daarmee

In hoeverre leidt de noodzaak tot controle van digitale dreigingen tot een meer gecentraliseerde, of juist meer gedecentraliseerde veiligheidszorg?

Om deze hoofdvraag te beantwoorden, wordt in dit multiple case-study onderzoek gewerkt met een tweetal op theoretisering gebaseerde hypothesen, waarvan de totstandkoming en toetsing via de beantwoording van de volgende deelvragen verloopt:

1. Wat valt er theoretisch gezien te verwachten ten aanzien van de gevolgen van digitalisering van dreigingen, op het gebied van veiligheidszorg?
2. Wat is er methodologisch gezien nodig om de hoofdvraag en empirische deelvragen te beantwoorden?
3. Wat zijn digitale dreigingen en hoe veranderen deze het algemene dreigingsbeeld?
4. Wat zijn de gevolgen van digitale dreigingen voor
    a. de organisatie, taken en verantwoordelijkheden van de politionele macht?
    b. de organisatie, taken en verantwoordelijkheden van de krijgsmacht?
    c. de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor private partijen (bedrijven)?
    d. de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor burgers?

Na beantwoording van deze deelvragen bestaat een duidelijk beeld van de rolverdeling ten aanzien van de totstandkoming van de veiligheidszorg ten aanzien van digitale dreigingen. Naar zal blijken leidt digitalisering tot een meer gedecentraliseerd veiligheidszorg. Deze conclusie noopt tot slot tot aanbevelingen voor vervolgonderzoek.

1.3 Wetenschappelijke en bestuurlijke relevantie

In de laatste jaren is het wetenschappelijk onderzoek naar digitalisering exponentieel gegroeid. 'Cyber' is *hot*, maar onderzoek beperkt zich vaak strikt tot het eigen vakgebied: onder meer in de informatica en aanverwante technische wetenschappen; economie; politicologie; bestuurskunde; filosofie; sociologie; en bedrijfskunde is onderzoek gedaan naar allerhande aspecten van digitalisering. Niet verwonderlijk; de wetenschappelijke, technologische en maatschappelijke impact van digitalisering is zodanig groot dat het ook wel geclassificeerd wordt als de vierde industriële revolutie[15].

Onderzoek naar de krijgsmacht en/of politionele macht is eveneens wijdverspreid. Er zijn reeds boeken en artikelen volgeschreven over trends van (re-)organisatie, centralisering en decentralisering bij de politie[16] en de krijgsmacht[17]; de rol van de krijgsmacht ten aanzien van

[15] zie bijvoorbeeld https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab

[16] zie bijvoorbeeld Treur (1998); Reiss Jr. (1992); en Wintle (1996);

[17] zie bijvoorbeeld Engelberts (1900).

interne dreigingen[18]; de verhouding tussen de krijgsmacht en de politionele macht[19]; de verhouding tussen de politionele macht en burgers[20]; de invloed van 'nieuwe' dreigingen op de veiligheidszorg door de politionele macht[21]; en talloze andere gerelateerde thema's. Een relatief onontgonnen gebied betreft de invloed van cyberdreigingen op de verhouding tussen krijgsmacht en politionele macht, of de invloed ervan op de (bestuurlijke) organisatie van de veiligheidszorg. Over de invloed van cyberdreigingen op de verhoudingen tussen de benen van de drieëenheid overheid - private partijen - burgers is wel al veel geschreven[22], maar tussen die geschriften bevinden zich betrekkelijk weinig wetenschappelijke publicaties.

Deze thesis springt in het gat dat nu nog bestaat tussen onderzoek naar digitalisering en onderzoek naar de (re-)organisatie van de traditionele veiligheidsapparaten. Dat is nodig omdat begrip van de causale mechanismen die tussen beiden werkzaam zijn, naast beter begrip van de werkelijkheid, zorgt voor mogelijkheden tot effectiever en efficiënter beleid ten aanzien van digitalisering. Bovendien wordt bijgedragen aan theoretisering omtrent de invloed van grote maatschappelijke en technologische veranderingen op de totstandkoming van veiligheidszorg. Dit onderzoek geeft immers inzicht in de manier waarop 'cyber' nou echt een *game-changer* vormt voor de veiligheidszorg ten aanzien van nationale veiligheid en openbare orde; hoe goed de krijgsmacht en politie in staat zijn om eigentijdse dreigingen te controleren; wat er van bedrijven en burgers verwacht wordt; en, als hoofdvraag, tot wat voor organisationele verandering deze dreigingen leiden. Eenduidige definities en 'conceptuele hygiëne' dragen bovendien bij aan een gestructureerde praktische aanpak, en zijn dus (naast wetenschappelijk relevant) van groot belang voor de bestuurlijke praktijk. Deze moet er immers voor zorgen dat de veiligheidszorg geleverd wordt door eigentijdse, flexibele bestuurlijke apparaten die 'mee' kunnen met belangrijke en onafwendbare technologische, bestuurlijke en maatschappelijke ontwikkelingen.

1.4 Leeswijzer

De volgende hoofdstukken zijn zodanig gestructureerd dat aan het eind van deze thesis via beantwoording van de deelvragen een tweetal hypothesen kan worden verworpen of aangenomen. Daarmee wordt automatisch de hoofdvraag beantwoord.

Het nu volgende hoofdstuk, het theoretisch kader, dient om op basis van bestaande wetenschappelijke theorievorming uit te leggen welke verwachtingen theoretisch gezien gesteld kunnen worden aan de rollen die de verschillende cases (krijgsmacht, politionele macht, bedrijven en burgers) ten aanzien van de veiligheidszorg in Nederland innemen. Dat gebeurt onder meer middels een historisch overzicht ten aanzien van de vier cases, tót 2012. In dat jaar vond middels de oprichting van de Nationale Politie een grote reorganisatie binnen de veiligheidszorg plaats. Ook nam het belang van digitale dreigingen in die periode een grote vlucht. In dat hoofdstuk wordt een tweetal hypothesen gepresenteerd, alsook een beoordelingskader. Hoe deze hypothesen getoetst worden, en welke overige methodologische keuzes zijn gemaakt, wordt besproken in hoofdstuk drie.

In hoofdstuk vier worden de data en bevindingen ten aanzien van de onafhankelijke variabele -de digitalisering van dreigingen- gepresenteerd en geanalyseerd, opdat een

[18] zie bijvoorbeeld Weger, de (2006) en Wal, van der (2004).

[19] zie bijvoorbeeld Dunlap Jr. (1999).

[20] zie bijvoorbeeld Kääriäinen & Sirén (2012).

[21] zie bijvoorbeeld Das et al., (2007).

[22] zie bijvoorbeeld https://www.computable.nl/artikel/expertverslag/overheid/6545362/4573232/cybersecurity-als-topprioriteit.html

genuanceerd overzicht geschetst wordt van de grote veranderingen die zich vanaf 2012 in het dreigingsbeeld hebben voorgedaan. Dit leidt tot de beantwoording van deelvraag 1. De analyse van data en bevindingen ten aanzien van de manier waarop de veiligheidszorg sindsdien tot stand komt, vindt plaats in hoofdstuk vijf. Dit leidt tot de beantwoording van deelvragen 2 tot en met 5. In het laatste hoofdstuk wordt vervolgens in de conclusie antwoord gegeven op de hoofdvraag, vindt reflectie op dit onderzoek plaats en wordt besproken hoe vervolgonderzoek eruit zou kunnen zien.

HOOFDSTUK TWEE
THEORETISCH KADER

In dit hoofdstuk wordt een veelheid aan relevante wetenschappelijke theorievorming en inzichten beschreven ten aanzien van de totstandkoming van veiligheidszorg. Het gaat voornamelijk om de rollen en verantwoordelijkheden van de cases die in dit onderzoek centraal staan: de krijgsmacht; de politionele macht; bedrijven; en burgers. Aan het eind van dit hoofdstuk leiden de gepresenteerde inzichten tot verwachtingen ten aanzien van de manier waarop de veiligheidszorg georganiseerd is, in het licht van digitalisering.

Ten gunste van duidelijke conceptualisering worden de kernbegrippen uit dit onderzoek besproken in de eerste paragraaf. Hierna volgt een historisch overzicht, waarin de totstandkoming van de rollen en verantwoordelijkheden, en golven van (de-)centralisatie ten aanzien van de vier cases besproken worden, tót 2012. Ten derde worden de relevante theoretische inzichten aangaande digitalisering van de samenleving besproken, en in welke mate dit een ontwikkeling betreft ten aanzien waarvan logischerwijs veranderingen in de totstandkoming van veiligheidszorg verwacht kunnen worden. Dit hoofdstuk sluit af met de presentatie van het conceptueel model en het tweetal hypothesen, op basis van enkele deelconclusies. Deze hypothesen betreffen direct ook de beantwoording van de eerste deelvraag van dit onderzoek.

2.1 Omschrijving kernbegrippen

2.1.1 Dreiging

Voor het concept 'dreiging' bestaat in de wetenschappelijke literatuur geen eenduidige, algemeen gangbare definitie. Enerzijds wordt in de recente literatuur niet eens gepoogd een definitie te geven[23]; men gaat direct over tot het classificeren van verschillende fenomenen, potentiële gebeurtenissen en zelfs personen als zijnde een dreiging voor het een of ander. Wat het concept 'dreiging' in die context precies inhoudt wordt in het midden gelaten en als min of meer bekend of logisch verondersteld. Anderzijds lopen opvattingen, definities en pogingen daartoe enorm uiteen; het is een zogenaamd *wezenlijk betwist begrip* (Cusumano & Corbe, 2018). Dit houdt in dat het concept dermate multi-interpretabel is dat niet tot een eenduidige conceptualisering gekomen wordt omdat de verschillende opvattingen erover te ver uit elkaar liggen (Gallie, 1956). In deze thesis wordt, vanwege de focus op de organisatie van de veiligheidszorg in Nederland, de conceptualisering van het begrip 'dreiging' aangehouden zoals dat in het Nederlandse openbaar bestuur gangbaar is. Het is belangrijk om daarbij aan te merken dat *perceptie* hier derhalve een belangrijke rol speelt.

Om de vier jaar brengt de Nederlandse overheid het zogenaamde Nationaal VeiligheidsProfiel (NVP) uit. Hierin wordt een all-hazard overzicht geboden van alle potentiële 'dreigingen die de Nederlandse samenleving kunnen ontwrichten', vanwege hun ernst en/of hun waarschijnlijkheid. Via de website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) wordt ten aanzien van het NVP gesteld dat[24]

[23] zie bijvoorbeeld: Tsirigotis, A. (2017). *Cybernetics, warfare and discourse : The cybernetisation of warfare in britain*. Cham, Switzerland: Palgrave MacMillan.

[24] https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/index.aspx

"de overheid wil voorkomen dat de maatschappij ontwricht raakt door een ramp of crisis. Daarom onderzoekt zij onder andere met de Strategie Nationale Veiligheid welke dreigingen de nationale veiligheid in gevaar kunnen brengen en wat we daaraan kunnen doen."

Uit deze omschrijving blijkt dat dreigingen worden gerelateerd aan het gevaar dat zij vormen voor de nationale veiligheid. In de Nationale Veiligheid Strategie van 2019 (NCTV, 2019b, p.15) stelt men dat er sprake is van een dreiging als sprake is van twee essentiële elementen:

"1. De Nederlandse vitale, ofwel nationale veiligheidsbelangen, dienen in het geding te zijn;
2. en de bedreiging van deze belangen dient dermate ernstig te zijn, dat sprake is van (potentiële) maatschappelijke ontwrichting."

De zes[25] nationale veiligheidsbelangen waarop gedoeld wordt, zijn als volgt omschreven:

Zes nationale veiligheidsbelangen
We onderscheiden de volgende nationale veiligheidsbelangen:

1. Territoriale veiligheid	Het ongestoord functioneren van Nederland en haar EU- en NAVO-bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin.
2. Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving.
3. Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie.
4. Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland.
5. Sociale en politieke stabiliteit	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden.
6. Internationale rechtsorde	Het functioneren van het internationale stelsel van normen en afspraken, gericht op internationale vrede en veiligheid.

[figuur 2.1 - De zes nationale veiligheidsbelangen. Bron: Nationale Veiligheid Strategie 2019]

De gemene deler van de zes belangen betreft de wens deze *ongestoord* te laten functioneren/voortbestaan. Dit betekent dat een potentiële ontwrichtende gebeurtenis of ontwikkeling ertoe leidt dat een situatie ontstaat waarin het gewone leven en de dagelijkse maatschappelijke gang van zaken geen doorgang kan vinden; deze is dan *verstoord*. Elke situatie, actor, ontwikkeling of gebeurtenis die de potentie heeft deze maatschappelijke normaalsituatie te verstoren verwordt daarmee tot een dreiging voor de nationale veiligheid[26]. Het ligt voor de hand dat er hier wel sprake moet zijn van een situatie die voor een dreiging op een bepaalde schaal (qua impact, schade, bereik etc.) vormt. Dreigingen op een te kleine schaal kunnen immers moeilijk gezien worden als bedreiging voor de nationale veiligheid. Een discussie over waar de ondergrens aan deze schaal ligt om te kunnen spreken van nationale aangelegenheid valt buiten het bereik van deze studie en stuit waarschijnlijk ook op het probleem dat het concept dreiging, zoals hierboven genoemd is, een *wezenlijk betwist begrip* is. Daar komt nog bij dat lokale of regionale gebeurtenissen regelmatig als maatschappelijk ontwrichtend gezien worden vanwege hun impact enerzijds, of vanwege hun mediagenieke karakter anderzijds(Cornelisse, 2011).

[25] In het NVP 2016 was nog sprake van vijf nationale veiligheidsbelangen. Internationale rechtsorde is de laatst toegevoegde.
[26] zie ook het nog te verschijnen WRR-rapport over digitale ontwrichting.

2.1.2 Interne en externe veiligheid.

Wat in de Nationale Veiligheid Strategie 2019 wordt omschreven als 'het ongestoord functioneren/voortbestaan van' de zes veiligheidsbelangen wordt door Brenner (2014) erkend als een noodzakelijkheid voor het het voortbestaan van welke menselijke samenleving dan ook: sociale orde. Zij onderscheidt vervolgens *interne* orde enerzijds en *externe* orde anderzijds, gebaseerd op de 'sfeer' van waaruit potentiële dreigingen voor de sociale orde zich manifesteren. Moderne menselijke samenlevingen hebben zich vooral via het concept van natiestaten georganiseerd, en de grenzen die het territorium van deze natiestaten afbakenen bepalen ook de scheidslijn tussen wat voor de betreffende samenlevingen als interne dreiging, en wat als externe dreiging kan worden gezien. Overheden van natiestaten hebben de verantwoordelijkheid voor het controleren van interne en externe dreigingen naar zich toe hebben door de claim op het monopolie op het legitieme gebruik van geweldsmiddelen. Externe dreigingen zijn daarmee een zaak van (interstatelijke) oorlogsvoering of -handelingen, en de externe veiligheid is dus de verantwoordelijkheid van krijgsmachten geworden; zij moeten burgers, belangen, territorium en zo meer beschermen tegen de oorlogshandelingen van andere staten. Interne dreiging betreft de ondermijning van de openbare orde door ontwrichtende activiteiten van sommige eigen burgers. Samenlevingen vertrouwen voor de controle van deze dreigingen in het algemeen op medeburgers die de nodige training hebben gehad en over wapens beschikken, wat heeft geleid tot het ontstaan van de politionele macht als verantwoordelijke voor de interne veiligheid.

2.1.3 Centralisatie en decentralisatie

Het klassieke debat over centralisatie versus decentralisatie gaat over de verdeling van verantwoordelijkheden en over responsabilisering[27]; de organisatie van de publieke sector en het wenselijke niveau waarop taken en verantwoordelijkheden ten aanzien van de totstandkoming van publieke diensten belegd worden.

Centralisatie betreft het door de staat uitstralen van politieke betrekkingen van en naar een centraal punt, om zo een territoriaal afgebakend gebied te beslaan waarover het een bepaalde mate van autoritaire, bindende wetgeving uitoefent, gesteund door georganiseerde strijdkrachten (Mann, 1993). Het kan als instrument voor politiek leiders gezien worden om een steviger grip te krijgen op de totstandkoming en uitvoering van beleid, op de coördinatie van uitvoerende departementen en instanties en op de controle op de daadwerkelijke uitvoer van beleid volgens de bedoeling van de beleidsmakers (Aucoin, 1999). Centrale organisatie kan als een theoretisch 'nulpunt' worden aangemerkt. Immers, er is pas decentralisatie mogelijk als er eerst sprake was van centralisatie (Hutchcroft, 2001).

Decentralisatie betreft het vergroten van de autonomie van lokale besturen en het overhevelen van -delen van- taken van de centrale overheid naar deze besturen, weg van de centrale overheid (Schneider, 2003). Het kan volgens economen leiden tot grotere efficiëntie, volgens politicologen tot gemakkelijker te organiseren democratische controle, en leidt volgens bestuurskundigen tot beter maatwerk (De Rynck & Wayenberg, 2013). Ook Schneider (2003) maakt onderscheid tussen decentralisatie op fiscaal, politiek en bestuurlijk gebied. Dit onderscheid dient in deze thesis als beoordelingskader, waarlangs in hoofdstuk 5 de bevindingen ten aanzien van de veiligheidszorg gelegd zullen worden. In dit beoordelingskader

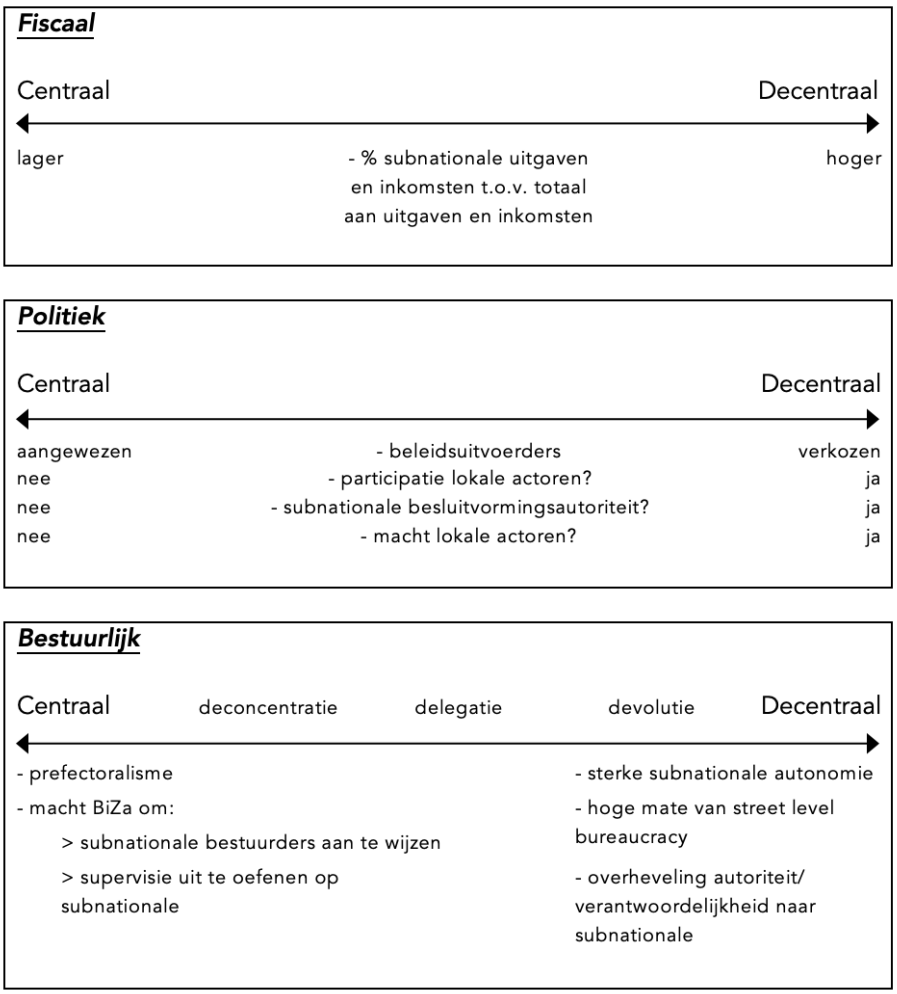
[27] zie bijvoorbeeld https://core.ac.uk/download/pdf/153396699.pdf

heeft *fiscale decentralisatie* betrekking op de mate waarin centrale overheden fiscale impact op decentrale overheden hebben, in termen van het percentage dat subnationale uitgaven en inkomsten uitmaken van het totaal aan uitgaven en inkomsten.

Politieke decentralisatie betreft de mate waarin centrale overheden decentrale actoren toestaan de politieke functies van bestuur te ondernemen, zoals mobilisatie, organisatie, participatie, vertegenwoordiging en belangenbehartiging. Gedecentraliseerde politieke systemen zijn die systemen waarbinnen politieke actoren en thematiek lokaal van belang kunnen zijn en ten minste gedeeltelijk onafhankelijk kunnen opereren van nationale politieke actoren en thematiek. Organisaties (zoals politieke partijen en sociale bewegingen) opereren lokaal en discussiëren over lokale thema's in lokale verkiezingen. Hutchcroft (2001) geeft aan dat indicatoren voor het indiceren van politieke decentralisatie zaken als het van bovenaf aanwijzen of van onderaf verkiezen van beleidsuitvoerders zijn, evenals de mate waarin lokale actoren onderdeel van besluitvormingsprocessen kunnen zijn; of er sprake is van een subnationale besluitvormingsautoriteit; en of er subnationale actoren met relatief grote machtsposities zijn.

Bestuurlijke decentralisatie betreft de hoeveelheid autonomie die decentrale actoren hebben, relatief aan centrale controle. Het gaat dan vooral om autonomie ten aanzien van hiërarchische structuren in het uitvoeren van beleid. Variërend van een beperkte hoeveelheid autonomie tot een vrij grote hoeveelheid autonomie worden in de literatuur (Hutchcroft, 2001; Schneider, 2003) gradaties onderscheiden (deconcentratie, delegatie en devolutie), maar dat betreft geen afgebakende categorieën: Schneider (2003) geeft aan dat deze gradaties eigenlijk niet veel meer zijn dan punten op een continuüm van bestuurlijke autonomie. Ter contrastering: een extreme vorm van bestuurlijke *centralisatie* wordt onder meer gekenmerkt door zaken als 'prefectoralisme' (waarbij het centrale gezag het territorium van een staat verdeelt in districten en een 'prefect' aan het hoofd van elk district plaatst. Deze prefect vertegenwoordigt die centrale overheid en is effectief dus een 'kleine koning' van het district, waarvan alle andere bestuurders en uitvoerders onder zijn gezag vallen); en een machtig centraal bestuursorgaan (meestal een Ministerie) dat beschikt over de capaciteiten om subnationale bestuurders en beleidsuitvoerders aan te wijzen en supervisie over hen uit te oefenen (Hutchcroft, 2001). Bestuurlijke *decentralisatie* kent daarentegen een sterkere mate van subnationale autonomie waarin ruimte bestaat om beleid naar eigen inzichten te maken, passend bij de subnationale omstandigheden. Daarnaast is er bij bestuurlijke decentralisatie sprake van overheveling van autoriteit en verantwoordelijkheid van de centrale overheid naar het subnationale niveau, en duidt ook een hoge mate van *street-level bureaucracy* op een hogere mate van bestuurlijke decentralisatie (Hutchcroft, 2001). Street-level bureaucrats zijn *"publieke dienstverleners die in hun werk direct met burgers interacteren, en die in de uitvoering van hun werk over substantiële handelingsvrijheid en beslissingsbevoegdheid beschikken"* (Lipsky, 2010, p.3). Zij kunnen bijvoorbeeld, gegeven de geldende normen en standaardprocedures, zelf inschattingen maken ten aanzien van de striktheid waarmee ze handhaven, aan welke cases al dan niet voorrang wordt verleend en op welke manier invulling geven aan beleid. Het is bovendien voor bestuurders bovenaan de hiërarchische piramide niet mogelijk om dergelijke 'lager-niveau' beslissingen in detail voor te schrijven; ze zijn te gecompliceerd om van bovenaf gereguleerd te worden (Vedung, 2015). Meer gecentraliseerde systemen zullen proberen middels de invulling van personele posities van bovenaf en strikte supervisie te zorgen voor zoveel mogelijk centrale invloed op street-level bureaucrats. Meer decentrale systemen zullen hen daarentegen juist meer bevoegdheden en autonomie geven, door beslissingsbevoegdheid naar subnationale niveaus te delegeren (Vedung, 2015).

Decentralisatie is een relatief concept; de bovenstaande dimensies en indicatoren moeten gemeten worden in termen van het aandeel dat de centrale overheid in het totaal heeft, omdat alle vormen van decentralisatie, ongeacht de ontvanger, betrekking hebben op het verschuiven van macht en hulpbronnen, weg van de centrale overheid (Schneider, 2003). Bovendien bevinden zich aan beide uiteinden van het continuüm theoretische extremen die in de echte wereld niet bestaan. Immers, totale decentralisatie zou een complete ontmanteling van de staat betekenen, en complete centralisatie zou de capaciteit van de staat om haar taken nog uit te kunnen voeren ernstig in gevaar brengen (Hutchcroft, 2001). De hierboven genoemde versies van, en indicatoren voor, (de-)centralisatie worden in onderstaand beoordelingskader (figuur 2.1) nogmaals op een rijtje gezet:



[figuur 2.2 - beoordelingskader (de-)centralisatie]

2.1.4 Overheid, voorschrift en gedrag

Nu duidelijk is welke opties overheden grofweg hebben om de organisatie van overheidsorganisaties vorm te geven (meer centraal versus meer decentraal), is het ook van belang te bezien hoe overheden zich verhouden tot hun samenlevingen, hoe zij deze trachten te besturen en welke veranderingen deze relatie tussen overheid en samenleving heeft ondergaan. Door oog te hebben voor trends en ontwikkelingen ten aanzien van manieren van besturen, kunnen immers uitingen van dat bestuur geduid worden.

De staat als overheidsvorm ontstond rond 1300 en maakte beslissende ontwikkelingen door tengevolge van de Westfaalse verdragen in 1648. Het proces kwam er grofweg op neer dat

machtige monarchen de heerschappij over afgebakende territoria claimden, en bestuurlijke macht bij en rondom zichzelf concentreerden. Om de militaire en civiele aspecten van die macht daadwerkelijk te kunnen gebruiken creëerden zij overheden (bureaucratieën) en infrastructuren van belastingen en communicatie. Deze overheden namen al gauw (delen van de) macht uit handen van de monarchen, waaruit 'de staat' daadwerkelijk werd voortgebracht (Van Creveld, 1999). Deze staten werden gekenmerkt door sterke centralisatie (Hutchcroft, 2001). De klassieke manier van besturen die staten er derhalve op nahielden kenmerkte zich door command-and-controlstructuren, hiërarchie, en het uitschrijven en handhaven van wet- en regelgeving om interne orde te creëren en onderhouden (Gruening, 2001). Een dergelijke, klassieke manier van besturen wordt gekenmerkt door een sterke mate van paternalisme; het uitoefenen van autoriteit 'van bovenaf' voor het begeleiden en ondersteunen van burgers en bedrijven, om voor de samenleving suboptimaal individueel gedrag te voorkomen. Het voorkomen van dergelijke suboptimaliteit werd (en wordt) geregeld midden wet- en regelgeving waarin middels verplichtingen en verboden gedrag wordt gestuurd (Heywood, 2017).

Moderne staten bereikten het hoogtepunt van hun klassieke command-and-control manier van bestuur tussen 1945 en 1975, toen van de welvaartsstaat verwacht werd dat deze voorzag in alle sociale en economische behoeften van burgers (Van Creveld, 1999; Osborne, 2010). Sindsdien is er sprake van een relatieve afname van de traditionele statelijke greep op zelfs de meest traditionele statelijke instituties zoals staatsbedrijven; systemen voor sociale zekerheid; het rechtssysteem; gevangenissen; publieke scholen; publieke omroepen; statistiekbureaus; en ook de krijgs-[28] en politiemachten[29]. Andere organisaties nemen (gedeeltelijk) de plaats van de staat in ten aanzien van de levering van allerhande publieke diensten. De klassieke manier van besturen maakte plaats voor wat ook wel 'New Public Management' wordt genoemd: een associatie van ideeën en componenten[30] die door voorstanders werd gezien als de enige manier om te corrigeren voor wat zij zagen als onherstelbare mislukkingen en amorele handelingen onder de klassieke manier van besturen (Hood, 1991). De opkomst ervan kon gekoppeld worden aan andere trends in het openbaar bestuur zoals het afremmen of zelfs omkeren van overheidsgroei (bureaucratisering (Wagenaar, 1997)) en de hang naar meer privatiseren, weg van traditionele, centrale overheidsinstanties. Zo werden het maken van beleid en de implementatie daarvan niet meer door dezelfde actor (de overheid) verricht, maar kwam de verantwoordelijkheid voor implementatie bij (elkaar beconcurrerende) private partijen te liggen. Er vond decentralisatie plaats, waardoor subnationale overheden een groter deel van het werk van de overheid gingen doen (Schneider, 2003). Ten aanzien van burgers en bedrijven ontstond een meer neoliberaal bestuur, waarin zaken als particuliere vrijheid en vrijheid om te ondernemen centraal staan en de rol van de overheid vooral het stellen van kaders om dat te stimuleren betreft (Harvey, 2007).

Met de schijnbare overgang naar NPM als dominant sturingsparadigma kwam er een stevige nadruk te liggen op efficiëntie, effectiviteit, overwegingen van geld en tijd, en daadwerkelijke output als het op de levering van publieke diensten aankwam (Hood, 1991). De focus die middels NPM gelegd werd op disaggregatie en onderlinge competitie zorgde er

[28] mondiaal zoeken krijgsmachten, nadat ze in omvang geslonken zijn na de Koude Oorlog, naar nieuwe missies zoals zoek- en reddingsacties en de aanpak van drugscriminaliteit.

[29] zoals nog zal blijken, nemen allerhande private organisaties en actoren politietaken voor hun rekening.

[30] NPM is een ruim begrip. Er is geen 'manifest' dat NPM afkondigde, vandaar dat het volgens Hood (1991) meer een clustering van ideeën en componenten betreft.

automatisch voor dat de hoeveelheid administratieve eenheden afnam en er tussen hen meer complexe, dynamische relaties ontstonden (Dunleavy et al., 2006).

NPM is echter slechts een tussenstation gebleken: het heeft er meer de schijn van dat NPM als een soort overgangsfase heeft gediend tussen het klassieke besturen en het staatsbestel dat Osborne *New Public Governance* (NPG) noemt[31]. NPG kenmerkt zich onder meer door de conceptie (en erkenning) van een meervoudige staat, waarbij meerdere wederzijds afhankelijke actoren in netwerken opereren en zo samen bijdragen aan de levering van publieke diensten (Osborne, 2010). Burgers en bedrijven interacteren met elkaar en met de overheid, en dragen bij aan de totstandkoming van publieke diensten die zij vervolgens ook weer zelf kunnen afnemen. Zo verwordt de rol van de overheid tot die van facilitator, tot één van de partners in het netwerk van maatschappelijke actoren die zorgen voor de productie van publieke diensten. Hierbij bedienen overheden zich dus in mindere mate van voorschriften als strikte wet- en regelgeving om gedrag te beïnvloeden. In plaats daarvan tracht men verstandig gedrag door bedrijven en burgers te stimuleren, door de randvoorwaarden te creëren die het gewenste gedrag zo gemakkelijk mogelijk maken: burgers krijgen bijvoorbeeld (in tegenstelling tot de situatie tijdens klassiek bestuur) de mogelijkheid hun eigen medische gegevens in te zien en hun eigen medische behandelingen mede vorm te geven; actief met hun eigen belastinggegevens en -aangiften aan de slag te gaan; hun eigen onderwijs mede vorm te geven en beleid voor hun eigen gemeenten en wijken mede te bepalen en uit te voeren (Dunleavy et al., 2006). In plaats van striktere wet- en regelgeving, te behalen prestatie-indicatoren en het uitschrijven van sancties wordt in steeds grotere mate gebruik gemaakt van gedragswetenschappelijk inzichten om middels 'nudges' -een 'duwtje in de goede richting'- gedrag te sturen zonder opties te verbieden of te sturen met economische prikkels[32].

De overgang van de klassieke manier van besturen naar NPG, via NPM als als overgangsfase, laat een afname van top-down, hiërarchische systemen zien, evenals een algemene beweging richting decentralisatie, vernetwerking en pluralisering.

2.2 Historisch overzicht; (de-)centralisatie en betrokkenheid

In deze paragraaf wordt het historisch overzicht geschetst waarbinnen de totstandkoming van de krijgs- en politionele macht als verantwoordelijken voor de veiligheidszorg heeft plaatsgevonden. Bovendien worden de verantwoordelijkheden van bedrijven en burgers ten aanzien van die veiligheidszorg door de geschiedenis heen besproken. Zoals zal blijken, is er sprake geweest van 'golfbewegingen' met betrekking tot centralisatie en decentralisatie, en de mate waarin bedrijven en burgers betrokken zijn bij de totstandkoming van veiligheidszorg. Deze golfbewegingen zijn steeds het gevolg geweest van maatschappelijke en technologische ontwikkelingen, en veranderende dreigingen.

2.2.1 Krijgsmacht

Krijgsmachten worden in traditionele optiek gekenmerkt door een hoge mate van organisationele centralisatie waarin autoriteit nauwelijks wordt gedeeld of overgedragen en er lager op de ladder nauwelijks ruimte is voor enige autonomie (Keren & Levhari, 1989). Toch is dergelijke strakke organisatie en hiërarchie niet altijd de norm geweest.

[31] hier is niet iedereen het mee eens. Hyndman & Liguori (2016) stellen bijvoorbeeld dat NPG helemaal niet zo alomtegenwoordig is als Osborne claimt. Zij constateren vooral NPM-ideeën en -componenten in het hedendaagse openbaar bestuur.

[32] zie bijvoorbeeld https://omooc.nl/wp-content/uploads/2016/11/Kamerbrief-Kabinetsreactie-op-adviesrapporten-MOOC-Slim-beleid-2016.pdf

Oorlog werd in de Middeleeuwen tussen de hogere klassen gevoerd (Van Creveld, 1999): zij hesen zichzelf in het harnas om elkaar met hun vazallen te bevechten wanneer de situatie daarom vroeg (voornamelijk vanuit overwegingen van eer en verplichting (Howard, 2009)). Toen in de dertiende eeuw ten gevolge van de herintrede van commerciële economieën mensen geld in handen begonnen te krijgen, ontsloegen heersers als koningen en prinsen hun vazallen van de verplichting voor hen te vechten, om in plaats daarvan beschermingsbelastingen van hen te innen. Met de opbrengsten hiervan konden de heersers huurlingenlegers aantrekken. Deze huurlingen namen tegen de tweede helft van de vijftiende eeuw het overgrote deel van de posities binnen de lagere rangen van hun feodale voorgangers over, en vormden daarmee private securityondernemingen die vochten voor de hoogste bieder (Howard, 2009). Het bouwen van een leger bestond voor een belangrijk gedeelte uit het in dienst nemen van troepen die gekleed, uitgerust en getraind moesten worden, alsook aangevoerd in oorlogssituaties (Van Creveld, 1999). De honderdjarige oorlog zorgde voor de grootste concentratie van dergelijke huurlingenlegers tot dan toe. In de periodes waarin de oorlog stil lag trokken ze echter rovend, verkrachtend en plunderend door het land. Om dit aan te pakken verordonneerde Charles VII van Frankrijk in 1444 dat een aantal van de plunderende huurlegers permanent diende te worden opgenomen in de koninklijke legers, die vervolgens werden ingezet om de resterende huurlingenlegers te ontmantelen (Howard, 2009). Zo professionaliseerden de krijgsmachten (die als de eerste moderne legers gezien konden worden), waarmee een einde kwam aan de oorlogen tussen prinsen en ridders, ten gunste van oorlogen tussen legers.

Bij de Dertigjarige Oorlog (1618-1648) waren de meeste Europese mogendheden van die tijd betrokken. Om te overleven dienden de huurlingenlegers te putten uit de burgerbevolking, die zich dientengevolge aansloot bij de huurlingenlegers. Dit leidde tot anarchische taferelen en zichzelf in stand houdend geweld, met uitzondering van de legers van de Republiek der Zeven Verenigde Nederlanden; deze werden regelmatig versterkt en betaald (Howard, 2009). Zo konden ze worden gedrild, getraind en geprofessionaliseerd. Hiertoe was echter wel een continue, niet-aflatende geldstroom nodig, wat het belang van grote private handelsondernemingen (zoals de VOC en WIC[33]) aanwakkerde[34].

Aan het eind van de Dertigjarige Oorlog, in 1648, werd de combinatie van religieuze overtuiging, zoektochten naar rijkdommen en de wens tot eerlijke handel die Europese expansiedrift en maritieme rivaliteiten 200 jaar lang had geïnspireerd middels de Westfaalse verdragen gesystematiseerd en gesimplificeerd tot conflicten tussen natiestaten (Howard, 2009). De verantwoordelijkheid voor het rekruteren, kleden, uitrusten, trainen en aanvoeren van troepen kwam te liggen bij ministeries van Oorlog (Van Creveld, 1999). De grote (voornamelijk Nederlandse, Engelse, Spaanse en Franse) handelscompagnieën bleven aanvankelijk echter als onafhankelijke actoren opereren en voerden naast handel ook oorlogen en vredesonderhandelingen. Dit eindigde in de achttiende eeuw, toen de oorlogsactiviteiten van deze ondernemingen ook onder statelijke controle kwamen. Tegen die tijd werden Europese oorlogen gevoerd door professionele krijgsmachten die begonnen te lijken op de hedendaagse legers. Militairen waren dienaren van de staat en met hun professionalisering (en uniformering) werd het mogelijk definitief een onderscheid te maken tussen de krijgsmacht en de burgers in een samenleving (Howard, 2009). De staat bood burgers een enorm verhoogd niveau van

[33] zie ook https://www.historischnieuwsblad.nl/goudeneeuw/artikelen/de-oorlog-van-de-voc-en-wic.html

[34] merk op: reeds toen ontstond een verhouding tussen private ondernemingen en het leveren van veiligheidszorg.

dagelijkse veiligheid in ruil voor de bereidheid zich op te offeren voor de staat wanneer men als dienstplichtige werd opgeroepen (Van Creveld, 1999). Daarbuiten werd de burgerij expliciet buitengesloten van de oorlogsvoering: dit onderscheid is één van de hoekstenen van de moderne samenleving.

Frankrijk zette de toon in het professionalisering van de krijgsmachtstructuur. Zij ontwikkelden een zodanig volledig functionerend militair mechanisme dat het door elke staat diende te worden geïmiteerd om er niet volledig door overwelmd te worden (Howard, 2009). Dit leidde ertoe dat veldslagen zeer destructief, en soldaten zeer moeilijk te vervangen waren. Het was daarnaast nog maar zelden nodig om frontlinie-soldaten in te zetten bij binnenlandse aangelegenheden. De meeste soldaten werden inmiddels uit de eigen burgerij gerekruteerd, en deze konden niet zomaar tegen medeburgers worden ingezet. De noodzaak ontstond om een onderscheid te maken tussen de krijgsmacht enerzijds en de politionele macht anderzijds (Van Creveld, 1999). Het ontstaan en de ontwikkeling van de politionele macht komt uitgebreid aan bod in paragraaf 2.2.2.

In het begin van de negentiende eeuw was oorlog niet langer synoniem voor handel en winst. Oorlogen werden uitgevochten door legers terwijl handel nagenoeg ongehinderde doorgang vond. Burgers en bedrijven dienden belastingen te betalen en ruimte te krijgen om geld te verdienen, en zich niet bezig te houden met oorlogsactiviteiten. Zij werden dus compleet buiten de totstandkoming van fysieke veiligheidszorg geplaatst. Betrokkenheid van welke 'derde' dan ook was een overtreding, en diende als zodanig veroordeeld en bestraft te worden. Het gebruik van geweld door 'mindere' actoren dan staten kreeg het predikaat van criminaliteit, opstand, rebellie of terrorisme (Van Creveld, 1999). De relatieve afstand van de burgerij tot oorlogsvoering veranderde echter door de uitvinding van de spoorwegen, aan het eind van de negentiende eeuw. De mogelijkheid om enorme aantallen soldaten in korte tijd te verplaatsen zorgde ervoor dat de veiligheid van een staat afhankelijk werd van de omvang (in aantallen) van de legers die zij konden produceren. Bovendien zorgde de toepassing van de telegraaf en heliograaf aan het eind van de 19e eeuw ervoor dat effectievere communicatie met (en dus coördinatie van) deze wijdverspreide troepen mogelijk was (Sterling, 2008). Dit leidde tot een enorme militarisatie van de Europese samenlevingen: oorlog was niet langer een aangelegenheid voor een afzonderlijke elite, maar van het hele volk. De krijgsmacht was de belichaming van de natie (Howard, 2009). Dit wordt onder andere levendig geïllustreerd door de volgende passage uit het opiniestuk 'De Reorganisatie onzer Landmacht' van W.M. Engelberts, geschreven in 1900 (p. 42, afwijkende opmaak niet in origineel):

> *"Wordt dan zoodra doenlijk voldaan aan den wensch in het Voorlopig Verslag uitgedrukt, "dat de Regeering de oefening der gymnastiek door de jeugd krachtig zal bevorderen, en ook het schijfschieten," ontwikkelt zich in de vereenigingen, die op enigerlei wijze de weerbaarheid van ons volk willen verhoogen een krachtig leven waaraan langen duur mag worden voorspeld; wordt in haar werken en streven éénheid en verband gebracht; neemt de lust merkbaar toe om deel te nemen aan voorbereidend militair onderricht, een en ander dank zij geldelijke steun der regeering, en toezegging aan militieplichtigen om korter onder de wapenen te mogen verblijven in de kazerne, naarmate zij blijk geven zich buiten de kazerne meer militaire eigenschappen en bekwaamheden te hebben verworven, dan kan binnen vijf jaar over het geheele land de noodige gelegenheid zijn open gesteld tot lichaams-, schiet-, en militaire oefeningen van allerlei aard naar een deugdelijk program, en zijn gegevens verkregen om te beoordeelen, of de thans goed te keuren wet op de nationale militie in dien zin kan worden gewijzigd, dat in snel tempo het militiecontingent jaarlijks grooter en het verblijf in de kazerne korter wordt, **totdat het Nederlandsche leger is geworden het gewapende Nederlandsche volk**, en de kazerne het gedwongen verblijf tot individueele oefening van hen, die zich er niet buiten tot weerbaar burger willen vormen."*

De totalitaire greep van oorlogsvoering op natiestaten veranderde weer door technologische ontwikkelingen halverwege de twintigste eeuw. Deze legden krachtige middelen (geavanceerde wapensystemen) in de handen van technisch bekwame militairen zowel op land, als op zee, als in de lucht. Met deze middelen konden oorlogshandelingen gericht worden tegen de ruggengraat van de vijandige natie; de bevolking. Binnen enkele jaren werden nucleaire wapens ontwikkeld. De angst slachtoffer te worden van aanvallen met dergelijke wapens (waartegen geen verdediging bestond) werd daarmee de belangrijkste reden voor staten om af te zien van het doorbreken van de vrede (Howard, 2009). Voor Nederland leidde dit er onder meer toe dat in 1996 de opkomstplicht voor dienstplichtigen werd afgeschaft; voortaan had Nederland een beroepsleger[35], waarin soldaten professionaliseren en zich specialiseren.

Bovenstaand overzicht in vogelvlucht van het ontstaan en de ontwikkeling van moderne krijgsmachten laat zien dat diens huidige vorm, waaraan hedendaagse samenlevingen gewend zijn, niet altijd al zo is geweest. De functie van, zeggenschap over, samenstelling van en organisatie van de krijgsmacht heeft enorme veranderingen ondergaan ten gevolge van veranderende dreigingen, technologische ontwikkelingen en economische omstandigheden. De fysieke, externe veiligheidszorg heeft bovendien een steeds centraler karakter gekregen; van losse, haast bij elkaar geraapte groepen krijgers tot een geprofessionaliseerd, strak aangestuurd beroepsleger.

2.2.2 Politionele macht

Het algemene beeld van de politie is dat deze in steeds verdere mate centraliseert (Koopman, 2013), en daarmee de *'odd one out'* is ten opzichte van de decentralisatietrend die algemeen gezien aan de gang lijkt te zijn. Zoals hierboven is genoemd, ontstond na 1700 de noodzaak om een strikt onderscheid te maken tussen de krijgsmacht en diens verantwoordelijkheden enerzijds, en de politionele macht anderzijds. Tot die tijd werd, ook in Nederland, de openbare orde min of meer gehandhaafd door (groepjes) individuen als nachtwachten, lantaarnopstekers, marktopzichters, boevenvangers, gevangenisbewaarders en andere, veelal private, actoren (Van Creveld, 1999; Wintle, 1996). Deze ordebewaarders waren semi-professionals met een zeer lokaal werkterrein. Dat politiewerk - het bewaren van de openbare orde en de omgang met wetsovertreders - vooral een private aangelegenheid was, is niet zo gek als het wellicht lijkt. Moderne politiekorpsen ontstonden in Frankrijk pas in de veertiende eeuw, en in Engeland niet eerder dan de negentiende eeuw (Dempsey & Forst, 2012). Bepaalde taken en verantwoordelijkheden die nu slechts een deel van modern politiewerk uitmaken, werden eerder al bij speciaal daartoe aangewezen personen belegd. Zo bestonden er in de vijfde eeuw vChr. in Rome speciale onderzoekseenheden voor moordzaken. In de zesde eeuw vChr. in Athene, en in de derde eeuw vChr. in Rome, waren magistraten als een soort rechters belast met het ten uitvoer brengen van wetten. Zij spraken recht, maar private burgers arresteerden en bestraften wetsovertreders (Dempsey & Forst, 2012). Rond het begin van de jaartelling stelde de Romeinse keizer Augustus vanuit het leger bepaalde groepen samen en dichtte hen de beveiliging van objecten als paleizen, belangrijke personen en de stad toe.

Gedurende de twaalfde en dertiende eeuw trokken Europese koningen de verantwoordelijkheid voor de tenuitvoerlegging van de wet naar zich toe. Ze namen daartoe wetsdienaren aan die de nachtwachten en andere private vormen van veiligheidszorg moesten vervangen. In Parijs benoemde Louis IX in de dertiende eeuw een zogenaamde provoost, die belast was met de tenuitvoerlegging van de wet en het toezicht op de nachtwachten. In 1356

[35] zie https://www.defensie.nl/onderwerpen/tijdlijn-militaire-geschiedenis/1990-2001-naar-een-expeditionaire-krijgsmacht

werd in Frankrijk de *Maréchausée* opgericht, destijds een quasi-militaire organisatie van ruiters die de orde op de grote wegen diende te bewaken. In de achttiende eeuw werd deze *Maréchausée* geassisteerd door lokale dorpsagenten en in Parijs door een speciale Parijse politie. Zij namen ook taken als het aansteken van straatlantaarns, brandblussen, afvalinzameling en dergelijke voor hun rekening (Stead, 1957). De *Maréchausée* is tijdens de Franse revolutie in 1789 en het daaropvolgende aan de macht komen van Napoleon Bonaparte geëvolueerd tot de *Gendarmerie Nationale* (centraal aangestuurd vanuit Parijs) (Hebenton & Thomas, 1995), die tegenwoordig de gebieden buiten de grote Franse steden onder haar hoede heeft (Dempsey & Forst, 2012). Nog steeds is deze organisatie een semi-militaire politiemacht, onderdeel van de Franse krijgsmacht.

In de twee decennia na 1810 richtte de ene na de andere staat in navolging van Napoleons Frankrijk nieuwe politiemachten op, en centraliseerden bestaande politiemachten. In Nederland werd het bestaande decentrale systeem van stedelijke en dorpse politie vervangen door het Napoleontische model tijdens de Franse annexatie van 1811-3 (Fijnaut, 1979; Hebenton & Thomas, 1995). Na het vertrek van de de Fransen werd hun *Gendarmerie* vervangen door de nationale militaire politie; de *Marechaussee*. De gemeentewet van 1851 voorzag daarnaast in de *Gemeentepolitie* en de *Rijkspolitie*. Deze situatie, met grofweg drie verschillende politieapparaten, hield vrijwel ongewijzigd stand tot de nieuwe politiewet van 1993 (Wintle, 1996)

De reorganisatie van de politionele machten in West-Europa kan volgens Fijnaut (1979) worden samengevat in één woord: nationalisering. Drie belangrijke kenmerken leiden naar deze conclusie. Ten eerste overzagen de opgerichte professionele politieapparaten op vrij uniforme manier het hele territorium van de staat. Ten tweede stonden deze politieapparaten ter beschikking van de nationale overheden, en ten derde werden zij onttrokken aan de directe controle van burgers; ze gingen over naar de staat. Dit zorgde voor een belangrijke versteviging van het geweldsmonopolie van nationale overheden.

In Groot-Brittannië verzette men zich tegen het Franse politiemodel. Politiewerk aldaar werd tot en met de achttiende eeuw verricht door een mix van sociale controle tussen groepen families, nachtwachten, agenten voor landelijke gebieden, sheriffs en zogenaamde 'Justices of the Peace' (JPs, vrij vertaald: vredebewaarders). De JP van Londen nam in 1750 een groep professionele boevenvangers in dienst om te assisteren bij het opsporen en arresteren van overtreders (Hebenton & Thomas, 1995).

Industrialisatie en de bijbehorende behoefte aan gedisciplineerde arbeidskrachten; onlusten en openbare ordeverstoringen; en maatschappelijke onrust ten gevolge van economische recessie en hoge voedselprijzen creëerden een vruchtbare voedingsbodem voor de oprichting en maatschappelijke acceptatie van formelere politionele macht. Zo werd in 1829 het eerste Engelse politiedepartement opgericht, de London Metropolitan Police. Deze politiemacht was een civiele, dus geen militaire, organisatie (Dempsey & Forst, 2012). In de jaren daarna spreidde politie-naar-Londens-voorbeeld zich uit naar andere Britse steden en uiteindelijk ook naar het platteland. Het grootste verschil met de sterk gecentraliseerde Franse politieorganisatie bestond uit de grote autonomie voor de verschillende lokale departementen; lokale agenten waren ongewapende burgers in een uniform, in plaats van quasi-militaire professionals. Als gevolg van de oprichting van de nieuwe politieorganisatie werd er afgestapt van het oude samenraapsel van private veiligheidssystemen dat tot die tijd werd gebruikt: centraler dan voorheen, maar decentraler dan het Franse politiemodel.

De oprichting van moderne politiekorpsen in Europa hebben met elkaar overeenkomstig dat ze het gevolg waren van collectieve verstoringen van de openbare orde.

Deze ordeverstoringen zorgden voor de vernieuwing van de politionele macht doordat zij zorgden voor een ernstige bedreiging voor de *"algemene verdeling van politieke macht"* die in Europa heerste (Fijnaut, 1979, p.595), en de bestaande politionele macht niet in staat was deze dreiging te controleren. Wat 'nieuw' is aan de *moderne* politiemachten van de achttiende en negentiende eeuw, wordt door Fijnaut (1979, p.580) als volgt omschreven:

> *"De verschijning van professionele politiekorpsen d.w.z. grote gehiërarchiseerde en gedisciplineerde gehelen van mensen die onder eenhoofdige leiding uitsluitend worden ingezet om actief en voortdurend op het gehele territorium van hun politieke overheid toezicht te houden en die hierbij speciaal tot opdracht hebben informatie te vergaren over alles wat de openbare orde raakt en zonodig snel kunnen worden samengetrokken om ernstige, collectieve verstoringen van deze orde te bedwingen. Deze korpsen kwamen in de plaats van een verbrokkeld, conflictueus, passief en zo ongeveer particulier politieapparaat en verdrongen leger en burgerwachten op het vlak van de ordehandhaving naar de tweede plaats."*

De nieuwe, allesomvattende aanwezigheid van de sterk gecentraliseerde politie leidde ertoe dat centrale overheden politieke beslissingen voor de bevolking bindend konden maken tot in de kleinste uithoeken van een staat, én konden handhaven (denk terug aan de bespreking van de klassieke manier van besturen volgens paternalistische principes, uit §2.1.4). Algemene verhoging van het niveau van algemene rust was het gevolg, doordat verstoringen van de openbare orde als dronkenschap, ruzies, losbandigheid en diergevechten niet meer werden getolereerd, evenals (collectief) geweld (Fijnaut, 1979). Om dit te beheersen was er sprake van een vergaande militarisering van de politionele macht (in organisatie, disciplinering en professionalisering), wat de inzet van het leger voor de handhaving van de openbare orde (zoals tot die tijd vaak nodig was) minder vaak nodig maakte. In Nederland gebeurde deze demilitarisering -de terugdringing van het leger uit de ordehandhaving- aan het eind van de negentiende eeuw. Hoewel het leger was teruggedrongen uit de ordehandhaving, werden wel militaire middelen en methoden door de politiekorpsen geadopteerd (Van der Wal, 2004). Hiermee ontstond dus een sterke scheiding tussen krijgsmacht enerzijds en politionele macht anderzijds; een scheiding waaraan dikwijls zeer veel waarde wordt gehecht, onder meer vanwege zeer verschillende werkwijzen ten aanzien van dreigingen (Van der Wal, 2004).

Aan het eind van de negentiende eeuw vond een aantal ingrijpende veranderingen in de organisatie van de Nederlandse politie plaats, uit angst voor verstoringen van de openbare orde door de opkomende socialistische arbeidersbeweging, onder invloed van de economische crisis van de jaren 1870. (Fijnaut, 1979). Vooral in het Noorden en Oosten van het land groeide de beweging, en dit ging gepaard met grote stakingen. De partij streefde de *"omverwerping der huidige maatschappelijke orde na*" (Fijnaut, 1979, p.960). De overheid reageerde door de Marechaussee in de noordoostelijke gebieden te vestigen. Later werden ook de rijksveldwacht (onderdeel van de Rijkspolitie) uitgebouwd en de rijksrecherche opgericht, en de Gemeentepolitie versterkt.

Met de politiewet van 1993 werden de gemeentelijke korpsen en het korps Rijkspolitie opgeheven en gereorganiseerd in 25 regionale politiekorpsen en het KLPD, wat een grotere centralisatie in de organisatie van de politie betekende, maar wel nog met een hoge mate van autonomie voor de regiokorpsen (Koopman, 2013). Twintig jaar later trad de Politiewet 2012 in werking waardoor de Nationale Politie werd opgericht en in plaats kwam van de regionale korpsen en het KLPD. De bestrijding van de zware en georganiseerde criminaliteit en terrorisme maakte één nationaal politiekorps noodzakelijk (Koopman, 2013).

Deze paragraaf laat een zeer beknopt overzicht zien van het ontstaan en de ontwikkeling van de Nederlandse politionele macht. Net als bij het ontstaan en de ontwikkeling van de krijgsmacht zijn veranderende dreigingen (zoals maatschappelijke onrusten) dikwijls een

belangrijke reden voor grote veranderingen in de organisatie, functie en maatschappelijke positie van de politie. Deze veranderingen hebben zich in andere landen op andere manieren voltrokken. Dat illustreert dat veranderende dreigingen en maatschappelijke ontwikkelingen niet enkel tot één-en-dezelfde uitkomst kunnen leiden. De manier waarop politionele machten veranderen ten aanzien van dergelijke ontwikkelingen lijkt derhalve meer een politieke overweging, dan een onontkoombaar gegeven.

2.2.3 Bedrijven

Ten aanzien van de moderne veiligheidszorg zijn we eraan gewend geraakt dat krijgs- en politionele macht zorgen voor bescherming tegen in- en externe dreigingen. Eerder in de geschiedenis zijn bedrijven ten aanzien van de veiligheidszorg -na golfbewegingen aan af- en toenemende betrokkenheid, met de VOC als hoogtepunt van betrokkenheid- reeds aan de 'ontvangende kant' geplaatst. Sinds de instelling van moderne politiemachten is het doen van politiewerk (*policing*) dus ook lange tijd uitsluitend de taak van de politie geweest. Tegenwoordig ligt dat genuanceerder. Het monopolie op de politiefunctie ligt al lang niet meer bij de traditionele vorm van politie. Cachet & Prins (2012) stellen dat vooral op lokaal niveau delen van de politiefunctie worden uitgevoerd door publieke (bv. gemeentelijke) toezichthouders, handhavers, stadswachten, boa's, stewards en private toezichthouders. *Policing* pluraliseert; het wordt nu verricht door meerdere *"zichtbare actoren voor misdaadbestrijding, door de overheid óf niet-overheidsinstanties"* (Jones & Newburn, 2002). Volgens Jones en Newburn (2002, p. 131) behelst die pluralisering drie hoofdpunten:

- *Er was een staatsmonopolie op politiewerk, maar dit is sinds het midden van de jaren '60 uiteen gevallen;*
- *Het bewijs hiervan ligt onder meer in het feit dat er nu drie keer zoveel private als publieke actoren zijn die politiewerk verrichten in de Verenigde staten, en twee keer zoveel in het Verenigd Koninkrijk. Die private veiligheidssector groeit daarnaast sneller dan de publieke politiesector;*
- *Het verrichten van politiewerk door 'anderen' -patrouilleringen, buurtwachten, misdaadpreventieassociaties, persoonsbeveiliging, en camera's rond scholen, winkelcentra en publieke parken- is van de sfeer van 'eigenrichting' naar een maatschappelijk geaccepteerd fenomeen ontwikkeld, zodanig dat de politie niet langer de primaire misdaadbestrijdende actor in de samenleving is.*

Bovenstaande brengt Bayley & Shearing (1996) ertoe te stellen dat het politionele monopolie op expertise binnen de eigen professie tot een eind is gekomen. *Policing*, en daarmee het bewaken van de openbare orde, is van iedereen geworden, in activiteit, in verantwoordelijkheid en in toezicht. Of dit inderdaad het geval is staat echter ter discussie en is afhankelijk van de manier waarop het concept 'monopolie' gedefinieerd wordt. De politie is de enige actor met het recht namens de staat te arresteren, vast te zetten en te chargeren, en pogingen dergelijke wettelijke bevoegdheden ook te verschaffen aan andere actoren in de samenleving stuiten op hevige weerstand (Jones & Newburn, 2002). De legitieme inzet van geweld voor de ordehandhaving blijft dus enkel in handen van de politie, maar voor heel veel traditionele politietaken die betrekking hebben op de interne veiligheid is dat inmiddels niet meer het geval. Shearing & Stenning (1983) leggen uit dat de groei aan private actoren die politiewerk verrichten zichtbaar is in bijvoorbeeld appartementencomplexen; op kantoren; in winkels en banken; in het openbaar vervoer of in sportstadions, universiteiten en ziekenhuizen. Bewaking door personen, camera's, sensoren en detectoren is inmiddels overal, doordat private beveiligingsactiviteiten zich ook naar het publieke domein hebben verplaatst. De bedrijven die deze beveiligingsdiensten bieden zien zichzelf bovendien niet als zogenaamde 'junior partner' van de

politionele macht, maar eerder als primaire actor in de veiligheidszorg, die door politie en justitie geholpen kan worden wanneer nodig.

Ten aanzien van de traditionele taken van de krijgsmacht, het leveren van externe veiligheidszorg, is er geen wetenschappelijke literatuur die beweert dat ándere actoren dan de krijgsmacht verantwoordelijkheid zijn gaan dragen voor de fysieke verdediging van het Nederlandse (of andere West-Europese) territorium, de staat en diens burgers. Voorstellen om de krijgsmacht deels op te laten gaan in een Europees leger stuiten bovendien op grote weerstand[36]. Wel wordt er melding gemaakt van zogenaamde *Private Military Companies* (PMCs) die in 'premoderne' of 'failed' staten een belangrijke, maar zeker niet onomstreden rol spelen in het beschermen of bedreigen van statelijke belangen (Leander, 2005). De veiligheidszorg in dergelijke staten valt echter buiten het bereik van deze studie, en hoewel dergelijke PMCs wel degelijk afkomstig kunnen zijn *uit* West-Europese staten (bijvoorbeeld het Verenigd Koninkrijk) en met vredesmachten kunnen samenwerken, opereren zij (voor zover bekend) niet *in of rond* West-Europese staten ter diens verdediging. Krijgsmachten hebben dus niet te maken met bedrijven die delen van hun traditionele takenpakket ten aanzien van fysieke veiligheidszorg overnemen, zoals bij de politionele macht het geval is.

2.2.4 Burgers

Op andere momenten in de geschiedenis was het voor burgers vrij normaal om onderdeel te zijn van de totstandkoming van de veiligheidszorg. De Angelsaksische *'fyrd'* was een lokale, Engelse defensiemacht rond het jaar 900 n. Chr., die bestond uit de *gehele* populatie van vrije mannen en die ter beschikking stond aan de koning, wanneer hij deze nodig had. Bewapening diende men zelf te regelen (Shaw, 1961). In een dergelijke situatie maken burgers een onmisbaar deel uit van de (lokale) veiligheidszorg. Deze betrokkenheid van burgers bij de totstandkoming van de veiligheidszorg heeft nogal gefluctueerd, zoals ook al uit bovenstaande paragrafen bleek. Waar burgers aan het eind van de negentiende eeuw tot halverwege de twintigste eeuw een belangrijke factor voor de toen gevoerde massa-oorlogen waren, is hen sindsdien steeds minder verantwoordelijkheid voor de nationale veiligheid toebedeeld: een beroep op burgers zoals voor de 'fyrd' gewoon was is nu ondenkbaar. Het lijkt ook niet meer nodig: overheidsinstellingen als krijgs- en politionele macht houden burgers nu veilig, in ruil voor het betalen van belastingen. Legendarisch is de uitspraak van toenmalig premier Colijn die enkele jaren voor de Tweede Wereldoorlog, toen Duitsland het Rijnland bezette, de woorden 'gaat u rustig slapen, de regering waakt over u' uitsprak[37]. Enkele jaren daarna bleek echter dat de oorlog niet zonder de betrokkenheid van burgers kon. Toch zijn de woorden van Colijn model komen te staan voor de huidige verhouding tussen overheid en burgers, die verwachten dat de overheid dreigingen beheerst en controleert[38]. Pieterman (2008) laat bovendien zien dat mensen überhaupt steeds minder bereid zijn risico's te accepteren, vooral in het geval van onvrijwillige blootstelling (Helsloot et al., 2010). Voor de meest uiteenlopende risico's kunnen mensen zich inmiddels verzekeren, opdat men in eventueel ontstane schade tegemoet wordt gekomen.

Verzekeringen tegen allerhande vormen van schade en pech eisen wel dat mensen tot op enige hoogte zorg dragen voor hun eigen veiligheid (bijvoorbeeld door eigendom in redelijke mate te beschermen tegen diefstal, door geen roekeloos gedrag te vertonen en door geen wetten

[36] zie bijvoorbeeld https://nos.nl/artikel/2280284-waarom-een-europees-leger-er-vooralsnog-niet-komt.html

[37] zie https://historiek.net/hendrikus-colijn-premier-crisisjaren/69176/

[38] zie https://www.volkskrant.nl/nieuws-achtergrond/met-gaat-u-rustig-slapen-red-je-het-niet-meer~bc924277/

te overtreden). Wet- en regelgeving is erop gericht gevaarlijke situaties zo min mogelijk te doen ontstaan en mensen tegen zichzelf en anderen in bescherming te nemen (bijvoorbeeld op het gebied van verkeersveiligheid). Dit alles maakt dat burgers zich bij uitstek aan de 'ontvangende kant' van de veiligheidszorg bevinden. Of dat een definitieve situatie is, valt echter niet met zekerheid te zeggen; de fluctuatie in (noodzakelijke) betrokkenheid van burgers bij de totstandkoming van veiligheidszorg is (wederom) te koppelen aan technologische en maatschappelijke ontwikkelingen. Immers, denk aan de invloed op hun betrokkenheid door de professionalisering van militairen en politieagenten, of de uitvinding van de spoorwegen en kernwapens. De huidige situatie zou heel wel kunnen veranderen indien een nieuwe technologische en maatschappelijke ontwikkeling zich voordoet, of in geval het dreigingsbeeld verandert.

2.3 Digitalisering als maatschappelijke en technologische ontwikkeling

Zoals inmiddels meermaals is gesteld, hebben maatschappelijke en technologische ontwikkelingen historisch gezien gezorgd voor veranderingen in de manier waarop veiligheidszorg tot stand is gekomen. Hier is geen recept voor; het soort ontwikkeling leidt niet per definitie tot centralisatie of juist decentralisatie. Ook kan niet gezegd worden dat per definitie vaststaat hoe de ontwikkeling de betrokkenheid van bedrijven en burgers in de totstandkoming van veiligheidszorg gaat beïnvloeden. Bovendien zijn er geen parameters gesteld aan de omvang van de ontwikkeling, wil deze van invloed zijn. De ontwikkelingen die hierboven genoemd zijn, en die dus door wetenschappers als belangrijke aanjager van veranderingen worden gezien, hebben echter wel overeenkomstig dat ze grote, (bijna) revolutionaire aangelegenheden vormen: de uitvinding van de spoorwegen; de uitvinding van nucleaire wapens; de opkomst van geavanceerde wapensystemen, industrialisatie, en de opkomst van het socialisme.

Momenteel is er sprake van een maatschappelijke en technologische ontwikkeling waarvan de impact zodanig is dat deze ook wel geclassificeerd wordt als de vierde industriële revolutie (Schwab, 2017): digitalisering. De Nederlandse samenleving en economie zijn sterk gedigitaliseerd[39], wat inhoudt dat steeds meer domeinen van de samenleving en economie zich structureren rondom digitale technologieën[40] (Brennen & Kreiss, 2016). Deze technologieën worden steeds geavanceerder en stellen 'alles' met elkaar in verbinding, zodanig dat inmiddels wordt gesproken van de 'digitalisering van bijna alles' (Brynjolfsson & McAfee, 2014). Van koelkasten tot auto's, en van broodroosters tot volledige 'smart cities'; alles waar een processor aan te pas komt staat via internet met elkaar in verbinding en dat verandert de manier waarop mensen leven, werken en interacteren ingrijpend (Schwab & Davis, 2018). Digitalisering, zo kan nu wel gesteld worden, is een revolutionaire technologische en maatschappelijke ontwikkeling die (naar zal blijken in hoofdstuk 4) onder meer zorgt voor een veranderend dreigingsbeeld. *Hoe* deze ontwikkeling zorgt voor verandering in de manier waarop veiligheidszorg tot stand komt, is het onderwerp van de rest van deze thesis. Hier volstaat het om aan te geven dat met het verplaatsen van bestaande, fysieke activiteiten naar het digitale domein, ook dreigingen van fysiek naar digitaal verplaatsen. De intrede van *cyberspace* als relatief nieuw medium waarlangs dreigingen voor de veiligheid zich kunnen materialiseren heeft volgens Anderson et al. (2013) via drie dimensies al dan niet gevolgen. Zo blijven ten eerste traditionele dreigingen voor de

[39] zie bijvoorbeeld https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2018/06/13/cybersecuritybeeld-nederland-2018-digitale-dreiging-neemt-toe/CSBN+2018.pdf

[40] Dit betreft de definitie van het engelse 'digitalisation', vaak gecontrasteerd met 'digitisation'; het simpelweg digitaal maken van analoge gegevens zoals papieren dossiers, foto's en filmbestanden

veiligheid (zoals oorlogshandelingen, spionage, criminaliteit en aanslagen) gewoon bestaan. 'Cyber' verandert dus niet 'alles'. Ten tweede kunnen bestaande, traditionele dreigingen zich geheel of gedeeltelijk verplaatsen naar de digitale wereld. Dit geldt bijvoorbeeld voor zaken als grootschalige fraude, de verspreiding van strafbaar materiaal, illegale handel, ondermijning, uitbuiting en afluisterpraktijken. Ten derde brengt de intrede van cyberspace dreigingen met zich mee die uniek zijn voor elektronische netwerken en informatiesystemen. *Distributed Denial of Service* (DDoS) aanvallen, de verspreiding van *SPAM* en malware en grootschalige hacks zijn hier voorbeelden van.

2.4 Deelconclusies, conceptueel model en hypothesen

De manier waarop publieke diensten worden geleverd kan fluctueren tussen een meer centrale of juist een meer decentrale aanpak, afhankelijk van fiscale, politieke en bestuurlijke aangelegenheden. De mate waarin decentrale actoren invloed kunnen uitoefenen op fiscale overwegingen, de invulling van belangrijke posities en beleidsrichtingen, en de mate waarin zij beschikken over autonomie in de taakuitvoering bepaalt in hoeverre de totstandkoming van publieke diensten als meer gecentraliseerd of meer gedecentraliseerd kan worden aangemerkt. Op basis van wat in dit hoofdstuk beschreven staat kan ten aanzien van de mate van (de-)centralisatie in de totstandkoming van de veiligheidszorg een aantal belangrijke stellingen worden geformuleerd:

1. De geschiedenis van moderne krijgs- en politionele machten laat zien dat diens huidige vorm, waaraan hedendaagse samenlevingen gewend zijn, niet altijd al zo is geweest. De organisatie van beide heeft enorme veranderingen ondergaan (in termen van (de-)centralisatie) ten gevolge van maatschappelijke en technologische ontwikkelingen, en veranderende dreigingsbeelden;
2. Ook de mate waarin bedrijven en burgers betrokken zijn geweest bij de totstandkoming van de veiligheidszorg heeft gefluctueerd, ten gevolge van maatschappelijke en technologische ontwikkelingen, en veranderende dreigingsbeelden;
3. Digitalisering is een revolutionaire maatschappelijke en technologische ontwikkeling, waarvan verwacht kan worden dat deze de manier waarop veiligheidszorg tot stand komt gaat beïnvloeden. Het leidt er onder meer toe dat dreigingen veranderen; ze verplaatsen zich geheel of gedeeltelijk naar het digitale domein. Ook ontstaan nieuwe dreigingen, exclusief ín het digitale domein.

Op basis van deze stellingen zijn er twee, aan elkaar tegengestelde, hypothesen mogelijk, die meteen de beantwoording van de eerste deelvraag van dit onderzoek betreffen. Theoretisch gezien kan ten aanzien van de gevolgen van digitalisering van dreigingen, op het gebied van veiligheidszorg het volgende verwacht worden: *ofwel* zet de hedendaagse *centralisatiestrend* in de veiligheidszorg zich door, *ofwel* leidt digitalisering tot verdere fragmentatie en pluralisering van de hedendaagse veiligheidszorg, en dus tot verdergaande *decentralisatie* daarvan. Deze verwachtingen staan schematisch weergegeven in onderstaand conceptueel model:

[figuur 2.3 - conceptueel model]

De pijlen in bovenstaand conceptueel model impliceren een positief, *one-way,* causaal verband tussen de betreffende variabelen. In woorden uitgeschreven gaat het hier dus om de volgende tegengestelde verwachtingen:

1. Hoe groter de mate waarin dreigingen digitaliseren, hoe meer *gecentraliseerd* de veiligheidszorg zal raken.
2. Hoe groter de mate waarin dreigingen digitaliseren, hoe meer *gedecentraliseerd* de veiligheidszorg zal raken.

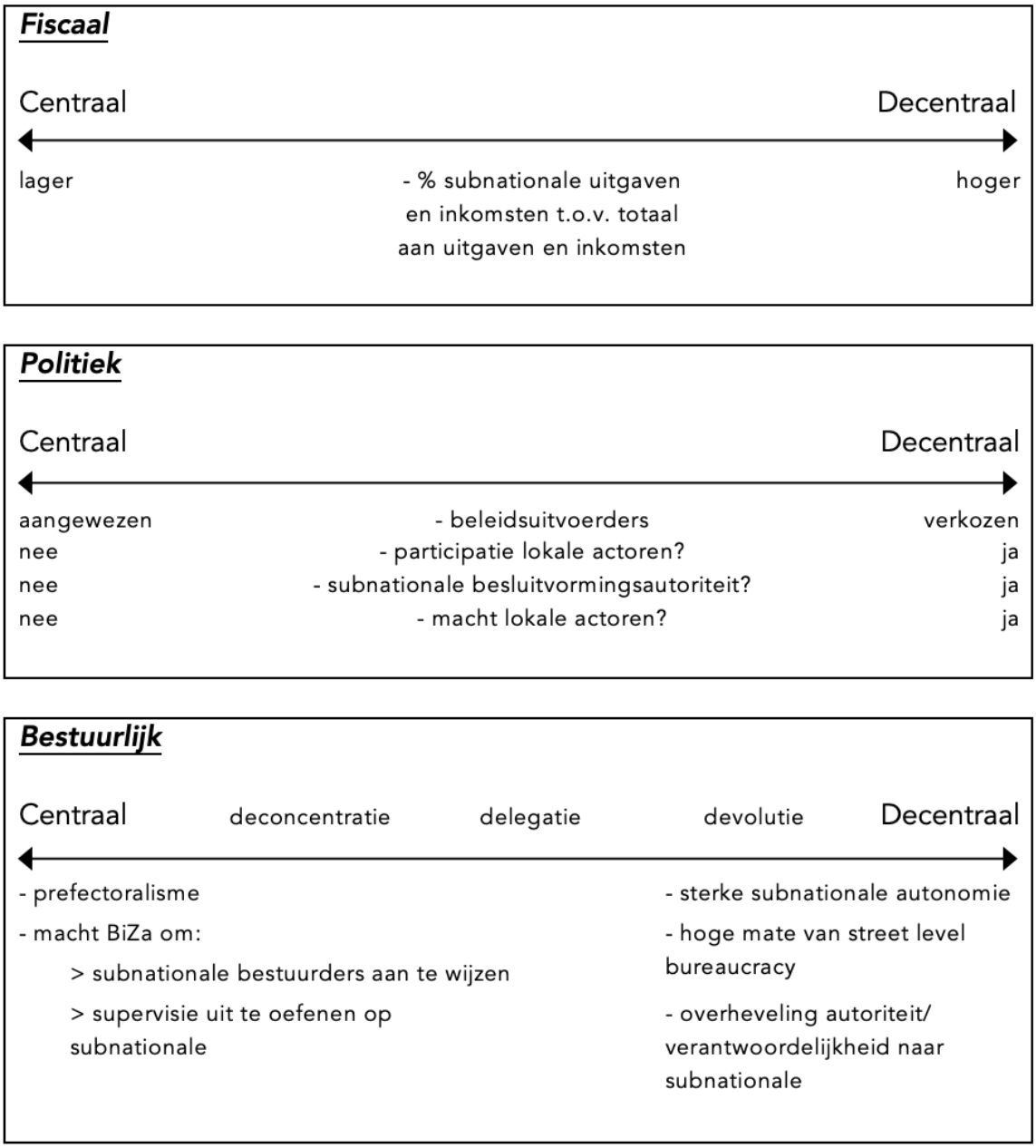
In het nu volgende hoofdstuk, het methodologisch hoofdstuk, worden de stellingen uit het conceptueel model geoperationaliseerd en wordt besproken op welke manier dit onderzoek verricht wordt.

HOOFDSTUK DRIE
METHODOLOGIE

In deze thesis wordt antwoord gegeven op de vraag '*in hoeverre leidt de noodzaak tot controle van cyberdreigingen tot een meer gecentraliseerde, of juist meer gedecentraliseerde veiligheidszorg?*'. De beantwoording van deze vraag ligt besloten in de acceptatie of verwerping van de twee hypothesen die aan het einde van het vorige hoofdstuk gepresenteerd zijn. De uiteindelijke acceptatie of verwerping van de hypothese verloopt via de beantwoording van de volgende deelvragen:

1. Wat valt er theoretisch gezien te verwachten ten aanzien van de gevolgen van digitalisering van dreigingen, op het gebied van veiligheidszorg?
2. Wat is er methodologisch gezien nodig om de hoofdvraag en empirische deelvragen te beantwoorden?
3. Wat zijn digitale dreigingen en hoe veranderen deze het algemene dreigingsbeeld?
4. Wat zijn de gevolgen van digitale dreigingen voor
    a. de organisatie, taken en verantwoordelijkheden van de politionele macht?
    b. de organisatie, taken en verantwoordelijkheden van de krijgsmacht?
    c. de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor private partijen (bedrijven)?
    d. de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor burgers?

De eerste deelvraag heeft geleid tot de hypothesen zoals die aan het eind van het vorige hoofdstuk gepresenteerd zijn. Het huidige hoofdstuk dient ter beantwoording van de tweede deelvraag. Uit de antwoorden op de derde en vierde deelvragen zal blijken in welke mate er sprake is van centralisatie, en in welke mate sprake is van decentralisatie van de veiligheidszorg ten aanzien van digitalisering van dreigingen. Hiertoe worden de organisatie van, en maatregelen door, krijgs- en politiemacht geanalyseerd, evenals het gedrag van, en voorschriften aan, bedrijven en burgers. Het hier verrichte onderzoek betreft een *toetsend, evaluatief multiple case-study onderzoek*: om de mate van centralisatie of decentralisatie te bepalen wordt gebruik gemaakt van het (op theorie gebaseerde) beargumenteerde beoordelingskader (uit §2.1.3), te vinden op de volgende pagina.



[figuur 2.2 - beoordelingskader (de-)centralisatie]

De evaluatie is tot stand gekomen op basis van een viertal case studies, waarin allerhande literatuur over de verschillende cases is geselecteerd en geanalyseerd, met de indicatoren uit het beoordelingskader hierboven, en de definities uit de tabel hieronder als leidraad. Deze definities worden hieronder verder geoperationaliseerd.

1. Dreigingen

1.1 Mate waarin sprake is van een gevaar voor minstens één van de zes nationale veiligheidsbelangen volgens zgn. monitoren, dreigingsbeelden en *threat assessments*

2. Digitalisering van dreigingen

2.1 Mate waarin sprake is van het verplaatsen naar cyberspace van bestaande/bekende gevaren voor één van de zes nationale veiligheidsbelangen

2.2 Mate waarin sprake is van nieuwe, zich volledig in cyberspace begevende gevaren voor één van de zes nationale veiligheidsbelangen

3. (De-)centralisatie t.a.v. digitaliserende dreiging

3.1 Mate van fiscale decentralisatie
- a. % subnationale uitgaven en inkomsten t.o.v. totaal aan uitgaven en inkomsten

3.2 Mate van politieke decentralisatie
- a. aangewezen of verkozen beleidsuitvoerders?
- b. mogelijkheden tot participatie lokale actoren?
- c. sprake van subnationale besluitvormingsautoriteit?
- d. relatieve positie lokale actoren?

3.3 Mate van bestuurlijke decentralisatie
- a. sprake van prefectoralisme of subnationale autonomie?
- b. sprake van machtig ministerie om bestuurders aan te wijzen en te superviseren?
- c. relatieve positie street-level bureaucrats?
- d. sprake van overheveling autoriteit/verantwoordelijkheid naar subnationale?

4. Private organisaties en burgers t.a.v. digitaliserende dreiging

4.1 Veranderende rol (relatieve toe-/afname) voor private partijen en burgers t.a.v. gedigitaliseerde dreigingen
- a. gedrag – wat doet men zelf?
- b. voorschriften vanuit overheid – wat wordt verwacht?

[box 3.1 – operationalisatie]

3.1 Discussie van de methode

Zoals gezegd betreft het hier verrichte onderzoek een *toetsend, evaluatief multiple case-study onderzoek*[41]. Voor dit onderzoeksontwerp is gekozen vanwege de aard van de onafhankelijke én afhankelijke variabelen die hier onderzocht worden. De digitalisering van dreigingen en de (de-) centralisatie van de veiligheidszorg zijn complexe, maatschappijbrede ontwikkelingen en organisationele aangelegenheden die zich het best laten vangen in het hier gebruikte onderzoeksdesign. Immers, een dergelijke methode is bij uitstek geschikt om complexe, unieke en specifiek situaties te analyseren, waarbij de grenzen tussen de onderzochte ontwikkelingen en de context waarin ze gebeuren niet altijd even helder zijn (Hakvoort, 1995).

[41] zie ook Hakvoort (1995)

De hier gebruikte onderzoeksmethode leent zich ten eerste voor het testen van de opgestelde hypothesen. George & Smoke (1974) stellen dienaangaande dat case studies zijn aan te raden voor het testen van theorie in de vorm *'als omstandigheden A optreden, dan volgt uitkomst B'*. Een dergelijke toetsing is hier aan de hand. Immers, uit het vorige hoofdstuk is de verwachting gebleken dat 'als maatschappelijke en technologische verandering/verandering van dreigingen optreedt, dit (de-)centralisatie van de veiligheidszorg ten gevolge heeft'. Ten tweede leent het verrichten van mutiple case study zich voor verkenning van de wisselwerking tussen digitalisering van dreigingen en de rol van maatschappelijke actoren. Deze wisselwerking doet zich, net als het digitaliseringsproces en de (re-)organisatie van overheidsorganisaties, voor 'in de echte wereld'; het betreffen real-life situaties met een sterkte contextgebondenheid. De onafhankelijke variabele (digitalisering van dreigingen) kan niet los worden gezien van die context, wat bijvoorbeeld het doen van onderzoek volgens experimenteel design minder waardevol maakt. Bovendien is niet gekozen voor het verrichten van survey-onderzoek vanwege praktische overwegingen: om representativiteit te garanderen zou binnen elke case een groot aantal eenheden dienen te worden verzameld, met als doel causaliteit al dan niet te kunnen bewijzen. Naast dat een dermate tijdrovende en kostenintensieve aangelegenheid is dat het de daartoe voor dit onderzoek beschikbare middelen overstijgt, is het middels het doen van survey-onderzoek moeilijker om inzicht te verkrijgen in specifiek de causale mechanismen en cross-case verbanden die juist zo belangrijk zijn voor dit onderzoek. Waar mogelijk en relevant, zijn in dit onderzoek wel secundaire bronnen gebruikt waarin survey-onderzoek is verricht. Tenslotte is vanwege dezelfde overwegingen aangaande beschikbare middelen niet gekozen interviews te gebruiken voor de uitvoering van dit onderzoek. Naast dat ook dit een tijd- en kostenintensieve onderzoeksmethode betreft, hebben andere overwegingen zoals de bereikbaarheid van de juiste (bewinds-)personen, managers en mogelijke bias onder de interviewees ertoe aangezet niet voor deze methode te kiezen. Ook hier geldt echter: waar mogelijk en relevant zijn wel secundaire bronnen gebruikt, waarin interviews en citaten van sleutelfiguren zijn opgenomen.

3.2 Selectie van cases

In dit onderzoek wordt een viertal cases onderzocht. Deze cases betreffen vier belangrijke partijen die in meer of mindere mate te maken hebben met de digitalisering van dreigingen, te weten de politionele macht; de krijgsmacht; private organisaties (bedrijven); en burgers. De eerste twee cases zijn de traditionele overheidsapparaten die belast zijn met de mitigatie van dreigingen voor de nationale veiligheidsbelangen. De laatste twee cases zijn juist (zoals besproken in het theoretisch kader) steeds meer op afstand komen te staan van de omgang met dergelijke dreigingen; ze worden er zo nu en dan wel door getroffen maar zijn in het algemeen niet verantwoordelijk voor de omgang met dreigingen voor de nationale veiligheidsbelangen.

De vier cases zijn gekozen, niet random geselecteerd, vanwege het kleine aantal partijen dat (op geaggregeerd niveau, dus niet individueel gesproken) te maken heeft met veiligheidszorg voor de nationale veiligheidsbelangen, ten aanzien van digitalisering. Uit de populatie van partijen die hier in meer of mindere mate mee te maken heeft (denk naast de vier hier onderzochte partijen onder meer aan de AIVD en MIVD, de Marechaussee en de FIOD), zijn de politie en leger *most-likely crucial cases*[42]; er wordt van de cases verwacht dat ze variatie op de afhankelijke variabele laten zien, gegeven de theorie dat maatschappelijke en technologische ontwikkelingen en veranderende dreigingen zorgen voor veranderingen in de organisatie van

[42] zie ook Gerring (2007).

veiligheidsapparaten. Als deze theoretisering inderdaad opgaat, moet er, gegeven de maatschappelijke en technologische ontwikkelingen en veranderende dreigingen die digitalisering tot gevolg heeft, iets veranderen in de organisatie van de krijgs- en politionele macht. Deze theorie wordt middels die hier uitgevoerde analyse dus getoetst.

Burgers en private organisaties zijn ook *most-likely crucial cases*; er wordt van deze cases ook verwacht dat ze variatie op de afhankelijke variabele laten zien. Dit is gebaseerd op de theorie dat interne veiligheid inmiddels niet meer enkel een zaak voor de politionele macht; dat externe veiligheid inmiddels niet meer enkel een zaak voor de krijgsmacht is; en dat digitalisering dit versterkt. Als dat waar is dan dient er, gegeven de maatschappelijke en technologische ontwikkelingen en veranderende dreigingen die digitalisering tot gevolg heeft, iets te veranderen in de rollen en verantwoordelijkheden die private organisaties en burgers (dienen te) nemen ten aanzien van de veiligheidszorg.

De verhoudingen tussen de cases (*cross-case*) worden diepgaand geanalyseerd, waardoor causale mechanismen inzichtelijk zijn gemaakt (zie ook 3.1 en 3.6). Echter, ook de cases zelf worden op verschillende niveaus geanalyseerd (op *within-case-evidence*); zo is bijvoorbeeld gekeken naar de complete organisatiestructuur van de krijgs- en politionele macht, maar is er ook aandacht voor verschillende decentrale niveaus, en wordt zelfs het individuele niveau van street-level bureaucrats besproken. Deze combinatie van *cross-case* en *within-case* analyse maakt de totale analyse van het geheel aan cases zo sterk mogelijk (Gerring, 2007).

De cases zijn geanalyseerd met betrekking tot de periode begin 2012-2019. Het startpunt van de analyse valt daarmee samen met de inwerktreding van de Politiewet 2012, die een rigoureuze reorganisatie van de politionele macht betekende. De periode tót 2012 staat voor alle cases beschreven in het historisch overzicht. Hoewel de eerste voorbeelden van digitale dreigingen zich reeds in de jaren '80 voordeden (Shackelford, 2018), heeft de Nederlandse overheid 'pas' in 2010 eerste Nationale Cyber Security Strategie (NCSS)[43] gepubliceerd. Daarop volgden onder meer het Nationaal Crisisplan ICT in 2012; de tweede NCSS in 2013, het Nationaal Veiligheidsprofiel 2016 (met 'cyber' nog al echte aparte dreigingscategorie); het Nationaal Handboek Crisisbesluitvorming 2016 (waarin de verantwoordelijkheid voor 'cyber' bij het NCSC belegd wordt, en verder niet benoemd); het CSBN 2017 en 2018. De echte 'wake-upcall' voor de Nederlandse overheid betrof de 'Diginotar-hack' van 2011; deze wordt ook wel de eerste Nederlandse digitale ramp genoemd[44]. Een jaar eerder, in 2010, werd middels de computerworm 'Stuxnet' het eerste 'cyberwapen' ooit door de VS en Israël tegen het Iraanse nucleaire programma ingezet[45]. Gegeven het feit dat in en rondom het jaar 2012 ten aanzien van de dreigingen die digitalisering met zich meebrengt dermate veel aandacht vanuit de overheid valt te constateren, en dit ongeveer samenvalt met de invoering van de Politiewet 2012, is dat jaar als startpunt voor de huidige analyse gekozen.

3.3 Selectie van de literatuur

Aangezien deze thesis hypothesetoetsend onderzoek betreft, dient er gestructureerd te werk te worden gegaan in de verzameling van de data (Hakvoort, 1995). Er zijn ten eerste publicaties gezocht die betrekking hebben op dreigingen, digitale dreigingen en de digitalisering van dreigingen, ongeacht de veroorzaker, doelwit of verantwoordelijke voor mitigatie. Er is

[43] zie https://www.nctv.nl/binaries/cyber-security-strategie_tcm31-32529.pdf en https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2009Z23494&did=2009D61723

[44] zie Van der Meulen (2013).

[45] zie bijvoorbeeld https://www.groene.nl/artikel/een-ballon-die-knapt

geselecteerd op publicaties die gepercipieerde dreigingen beschrijven voor de interne en/of externe orde. Ten tweede zijn er publicaties gezocht die betrekking hebben op een viertal partijen: de politionele macht; de krijgsmacht; private partijen (bedrijven); en burgers. Bovendien hebben deze publicaties betrekking op dreigingen in het algemeen, en/of digitalisering van dreigingen specifiek.

De publicaties, in het Nederlands en het Engels, zijn via de sneeuwbalmethode gezocht via de volgende wegen, tot inhoudelijke verzadiging optrad:

- Internet in het algemeen (met Google als zoekmachine), en meer specifiek op websites van ministeries en overheidsinstellingen, wetenschappelijke onderzoeksinstellingen (WRR, Rathenau, TNO, AIV, Clingendael);
- Google Scholar;
- RUQuest;

De daadwerkelijke selectie van de publicaties is vervolgens tot stand gekomen middels de volgende criteria:

- Kwaliteit van de bron, op rangorde van boven naar beneden:
    - wetenschappelijke publicaties, beleidsstukken en wetten (artikelen en boeken);
    - rapporten van gerenommeerde onderzoeksinstituten (WRR, Rathenau, TNO, AIV, Clingendael);
    - rapporten van overheidsinstellingen, geïnitieerd of gesubsidieerd door de overheid;
    - secundaire data;
    - rapporten van bedrijven of gesubsidieerd door bedrijven;
    - nieuwsberichten;
    - overige publicaties (Blogs, opiniestukken, videomateriaal etc.).

  De weging van de bron is afhankelijk van de betrouwbaarheid en validiteit ervan.
- Wetenschappelijke betrouwbaarheid (op basis van methoden, type en hoeveelheid data);
- Actualiteit, waarbij het criterium 'recenter maakt bruikbaarder' is gehanteerd;
- Relevantie, waarbij het criterium 'relevanter maakt bruikbaarder' is gehanteerd. Maar: als een publicatie ouder maar relevant is, is deze geselecteerd ondanks het jaartal.

Uiteindelijk is gekomen tot een verzameling van literatuur die bestaat uit wetenschappelijke publicaties; 'dreigingsbeelden'; overheidspublicaties zoals monitors, profielen en rapporten.

3.4 Analyse van de cases

De geselecteerde publicaties over de krijgsmacht en politionele macht zijn middels kwalitatieve-interpreterende inhoudsanalyse[46] geanalyseerd. Ten eerste heeft analyse plaatsgevonden op (al dan niet bestuurlijke) maatregelen -die handelingen die verricht worden door overheidsinstellingen om dreigingen (algemeen) en digitale dreigingen (specifiek) te mitigeren of om er beter mee om te kunnen gaan. De maatregelen die betrekking hebben op rolverdelingen, verantwoordelijkheden, onderlinge verhoudingen en dergelijke tussen de vier in deze thesis besproken cases, zijn geselecteerd.

Vervolgens zijn de publicaties over de krijgsmacht en politionele macht geanalyseerd ten aanzien van fiscale decentralisatie, politieke decentralisatie en bestuurlijke decentralisatie. Hierbij is centraliteit het uitgangspunt, dus beschreven wordt de mate waarin er van centraliteit wordt afgeweken. Dit wordt beoordeeld aan de hand van het beoordelingskader (zie het begin

[46] zie https://repository.ubn.ru.nl/bitstream/handle/2066/56967/56967.pdf

van dit hoofdstuk). Dit kader beschrijft de indicatoren die gebruikt worden om te bepalen of er sprake is van meer centraal, of meer decentraal beleid.

Voor de andere twee cases -private bedrijven en burgers- is de verzamelde literatuur (ook op kwalitatieve-interpreterende wijze) geanalyseerd op informatie betreffende gedrag (*wat doen bedrijven zelf en wat doen burgers zelf?*) en betreffende voorschriften vanuit de overheid (*wat wil de overheid dat bedrijven doen en wat wil de overheid dat burgers doen?*). Hierbij is als volgt gewogen: hoe meer verantwoordelijkheden, taken, autonomie en dergelijke vanuit voorschriften of gedrag bij burgers en/of bedrijven (zijn) komen te liggen, hoe decentraler[47]. Hoe meer verantwoordelijkheden, taken, autonomie en dergelijke vanuit voorschriften en gedrag bij burgers en bedrijven zijn weggehaald (en bij meer centrale niveaus zijn ondergebracht), hoe centraler.

Het eindoordeel ten aanzien van centralisatie en/of decentralisatie van de veiligheidszorg ten aanzien van digitalisering is vervolgens via twee stappen tot stand gekomen. Ten eerste is per case beargumenteerd afgewogen of er, *absoluut gezien*, een groter, kleiner of gelijk deel van de veiligheidszorg ten aanzien van digitalisering van dreigingen voor diens verantwoordelijkheid is gekomen. Dit gebeurt door de huidige situatie te vergelijken met hoe deze voorheen was (eventuele verandering moet blijken uit de maatregelen die zijn getroffen en/of organisationele veranderingen die hebben plaatsgevonden). *'Voor'* en *'na'* worden gedefinieerd door de hier aangehouden tijdspanne: de situatie vóór 2012 en de situatie vanaf 2012. Ten tweede is de relatieve positie van cases ten opzichte van elkaar in ogenschouw genomen. Het betreft dan de *relatieve* rol in het leveren van veiligheidszorg als publieke dienst, door vast te stellen of er sprake is van overheveling van taken, verantwoordelijkheden en dergelijk van de ene naar de andere partij.

3.5 Toetsing van de hypothesen

Hypothese 1 (H1)[48] *'hoe groter de mate waarin dreigingen digitaliseren, hoe meer gecentraliseerd de veiligheidszorg zal raken'* wordt geaccepteerd indien ten aanzien van de digitalisering van dreigingen bevoegdheden, verantwoordelijkheden en autonomie van decentrale niveaus naar het centrale niveau blijken te zijn overgeheveld. In dat geval kan er immer een dynamiek van decentraal naar centraal worden vastgesteld. Hypothese 2 (H2) *'hoe groter de mate waarin dreigingen digitaliseren, hoe meer gedecentraliseerd de veiligheidszorg zal raken'* zal worden geaccepteerd indien er sprake is van eenzelfde dynamiek, maar dan van centraal naar decentraal.

Acceptatie van één van beide hypothesen sluit acceptatie van de andere hypothese niet automatisch uit. Er is derhalve een mogelijkheid dat beide hypothesen worden geaccepteerd. Aangezien centralisatie of decentralisatie een 'beweging' impliceert (zie ook §2.1.2), worden beide hypothesen verworpen indien er geen sprake is van enige beweging richting centraliteit of decentraliteit. In dat geval blijkt dat er ten aanzien van de digitalisering van dreigingen op geen enkele manier een overheveling van taken, verantwoordelijkheden of autonomie plaatsvindt. Indien bij alle vier de partijen een toename in verantwoordelijkheden en taken wordt geconstateerd, zou er sprake kunnen zijn van een 'groei' van veiligheidszorg ten aanzien van digitalisering.

[47] denk hierbij aan overwegingen met betrekking tot de digitale weerbaarheid van deze groepen, digitale skills, de eigen inschatting ten aanzien van verantwoordelijkheden en de bereidheid daarnaar te handelen.

[48] aangezien het hier geen kwantitatief, statistisch onderzoek betreft, is niet de daar gangbare benaming H0 (nulhypothese) en H1 (alternatieve hypothese) aangehouden. Deze zouden elkaar immers moeten uitsluiten, en dat is hier niet het geval.

3.6 Validiteit en betrouwbaarheid

Case study-onderzoek kenmerkt zich door een hoge mate van interne validiteit door de aandacht die er is voor causale mechanismen en diepgaand, gedetailleerde analyse. Het gebruik van meer cases verhoogt deze bovendien (Hakvoort, 1995). Omdat er gedetailleerd, *within-case* en *cross-case* onderzoek wordt verricht, zijn de uiteindelijke bevindingen zeer representatief te noemen voor de onderzochte cases. De opgestelde hypothesen laten bovendien een verwachting zien; wanneer de hypothesen kunnen worden aangenomen versterkt dit de theorie waaruit de hypothesen zijn voortgevloeid.

De externe validiteit ligt bij case study-onderzoek doorgaans niet bijzonder hoog. Immers, het is moeilijk om vanuit een beperkt aantal cases inductief te werk te gaan (Gerring, 2007). Zoals hierboven reeds gemeld, is de totale populatie van partijen die (op geaggregeerd niveau, dus niet individueel) te maken hebben met veiligheidszorg voor de nationale veiligheidsbelangen, ten aanzien van digitalisering, beperkt. Ze zijn bovendien vrij specifiek en slechts op bepaalde factoren vergelijkbaar. Derhalve kan met de uiteindelijke bevindingen uit deze thesis nauwelijks uitspraken gedaan worden over organisaties als de AIVD, MIVD, Marechaussee en FIOD. Omdat hier echter op een dermate geaggregeerd niveau analyse wordt verricht, valt het te verwachten dat voor ándere krijgs- en politionele machten, private sectoren en burgerijen wel inductief te werk kan worden gegaan. Immers, hoewel er variatie bestaat tussen landen waar het gaat om de organisatie van politionele macht (zie ook het vorige hoofdstuk), kan ook voor deze partijen verwacht worden dat zij in meer of mindere mate (de-) centraliseren ten aanzien van de digitalisering van dreigingen. Bovendien kunnen de uiteindelijke bevindingen uit de huidige analyse worden gebruikt om een verwachting te stellen ten aanzien van toekomstige technologische en maatschappelijke ontwikkelingen, veranderende dreigingen en de gevolgen die dat heeft voor de organisatie van de veiligheidszorg.

'Betrouwbaarheid' ten aanzien van kwalitatief onderzoek wordt doorgaans geconceptualiseerd als 'waarachtigheid' (*trustworthiness*), grondigheid en kwaliteit. Om dit te bereiken dienen bias en eenzijdigheid zoveel mogelijk te worden voorkomen middels het gebruik van zoveel mogelijk verschillende (qua opzet, methode, herkomst etc.) bronnen van informatie; triangulatie (Golafshani, 2003). Zoals besproken in §3.2 is dientengevolge getracht vanuit zoveel mogelijk verschillende hoeken bronnen van verschillende aard, in twee verschillende talen en vanuit verschillende vakgebieden te selecteren. Waar mogelijk en relevant is bovendien steeds verwezen naar zoveel mogelijk bronnen die een bepaalde stelling of overtuiging onderschrijven, opdat zij elkaar ondersteunen.

HOOFDSTUK VIER
EEN VERANDEREND DREIGINGSBEELD

Het conceptueel model voor deze thesis hanteert 'digitalisering van dreigingen' als onafhankelijke variabele. Dit hoofdstuk dient om deze variabele grondig te analyseren, teneinde de derde deelvraag, 'wat zijn digitale dreigingen en hoe veranderen deze het algemene dreigingsbeeld?' te kunnen beantwoorden.

In hoofdstuk 2 is reeds duidelijk gemaakt dat maatschappelijke en technologische ontwikkelingen, alsook veranderende dreigingen, vaak reden geven tot organisationele veranderingen ten aanzien van de totstandkoming van in- en externe veiligheidszorg. Het idee dat digitalisering gezien kan worden als revolutionaire maatschappelijke en technologische ontwikkeling, leidde tot de verwachting dat dit wederom tot veranderingen in de totstandkoming van de veiligheidszorg kan leiden. In dit hoofdstuk wordt de invloed van digitalisering op het algemene dreigingsbeeld voor de nationale veiligheidsbelangen geschetst. Naar zal blijken wordt de rol van digitalisering gekenmerkt door dualiteit: enerzijds is digitalisering één van de factoren in een überhaupt veranderend dreigingsbeeld. Anderzijds is digitalisering juist een aanjagende factor van deze verandering in het dreigingsbeeld. Vanzelfsprekend is het lastig om een kwantitatieve inschatting van een verandering in dreiging te maken, maar naar zal blijken is de perceptie ten aanzien van digitale dreigingen duidelijk veranderd.

De eerste paragraaf van dit hoofdstuk dient om de veranderingen aangaande het dreigingsbeeld ten aanzien van de nationale veiligheidsbelangen inzichtelijk te maken. In de tweede paragraaf wordt vervolgens de duale rol van digitalisering ten aanzien van dit veranderende dreigingsbeeld besproken. Aan het eind van die tweede paragraaf kan de derde deelvraag van dit onderzoek beantwoord worden.

4.1 Dynamiek en vervlechting

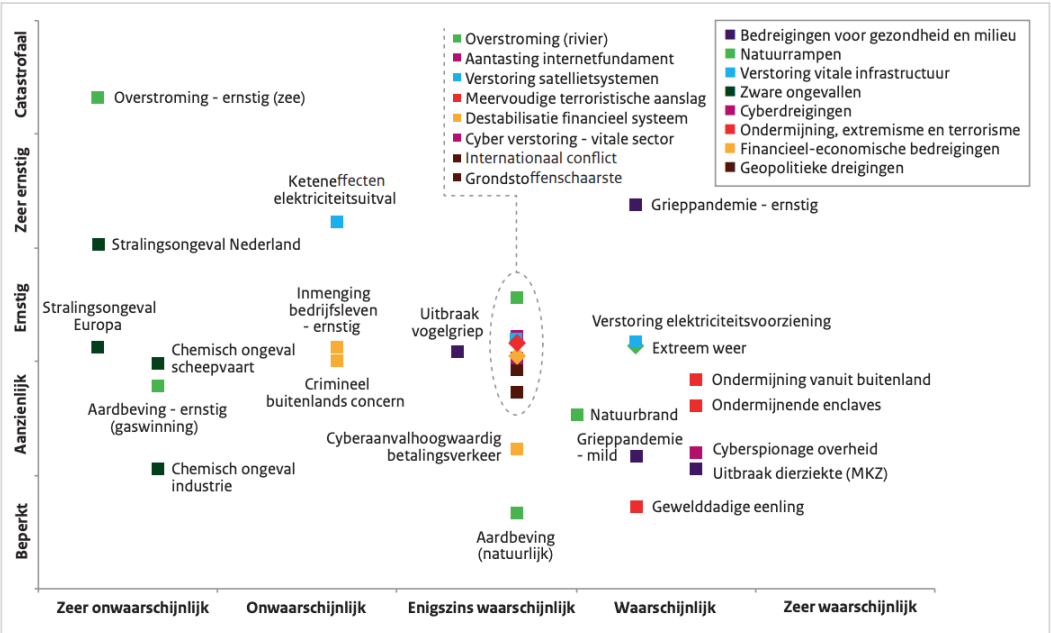
De Rijksoverheid publiceert reeds enkele jaren een veelvoud aan zogenaamde dreigingsbeelden, dreigingsmonitoren, horizonscans en veiligheidsstrategieën. In hoofdstuk 2 is reeds het Nationaal Veiligheidsprofiel 2016 kort aan bod gekomen. Na die tijd volgden onder meer nog de Horizonscan Nationale Veiligheid (2018); de Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022; de Dreigingsbeelden Terrorisme Nederland 42 t/m 50; en een zestal Risico- en Crisisbarometers. Ten aanzien van de interne veiligheid wordt de Strategie Nationale Veiligheid gepubliceerd, en voor de externe veiligheid is er de Internationale Veiligheidsstrategie. Ook andere organisaties publiceren toonaangevende rapporten om dreigingsbeelden te schetsen; onder meer Clingendael, Europol en het World Economic Forum hebben hun eigen publicaties op dit gebied. De meeste van al deze publicaties richten zich op specifieke dreigingen of domeinen die met dreigingen samenhangen, zoals terrorisme, veiligheidsgevoelens van Nederlanders, en de internationale aanpak voor de veiligheid van Nederlanders en Nederland. In deze publicaties is het gebruikelijk onderscheid te maken tussen verschillende soorten categorieën van dreigingen, vaak 'de meest urgente veiligheidsdreigingen' genoemd. Voorbeelden van dergelijke dreigingscategorieën, uit de verschillende publicaties, zijn

- (extremistische) terroristische aanslagen;
- ongewenste buitenlandse inmenging en ondermijning
- militaire en/of geopolitieke dreigingen;

- bedreiging van vitale (al dan niet economische) processen en/of infrastructuur;
- dreiging van chemische, biologische, radiologische en nucleaire middelen (CBRN);
- natuurrampen;
- bedreigingen gezondheid en milieu;
- zware ongevallen;
- cyberdreigingen;
- financieel-economische dreigingen.

Al deze dreigingscategorieën zijn als zodanig onderscheiden omdat zij de potentie hebben het normale maatschappelijk leven zodanig te verstoren dat (een van) de nationale veiligheidsbelangen in het geding zijn. Verschillende publicaties bedienen zich ook van het sorteren van deze dreigingscategorieën naar waarschijnlijkheid en impact, zodat een vorm van prioritering kan plaatsvinden en (de ernst van) dreigingen onderling vergeleken kunnen worden. Dat levert diagrammen op zoals onderstaand (figuur 4.1), uit het Nationaal Veiligheidsprofiel 2016:

Risicodiagram met daarin de scenario's die als illustraties bij de dreigingsthema's dienen.



[figuur 4.1 - dreigingsdiagram (Bron: Nationaal Veiligheidsprofiel 2016 (NCTV, 2016))]

Welke dreigingen het meest prangend zijn, kan binnen korte tijd compleet verschillend zijn. Het *Global Risks Report 2018* van het World Economic Forum laat zien hoe in een betrekkelijk korte tijd de dreigingsdynamiek compleet kan veranderen. Waar in het begin van de afgelopen tien jaar voornamelijk economische, geopolitieke en maatschappelijke dreigingen waarschijnlijk werden geacht, is dat zodanig veranderd dat tegenwoordig vooral ecologische, technologische (en in mindere mate maatschappelijke en geopolitieke) dreigingen waarschijnlijk zijn.

Het categoriseren en qua waarschijnlijkheid en/of impact tegen elkaar afzetten van dreigingen mag beleidsmatig of gevoelsmatig voordelen met zich meebrengen, het doet geen recht aan de praktijk. Dreigingen hangen immers met elkaar samen en zijn in potentie zelfs elkaars gevolg (Li et al., 2010). Ter illustratie: in Japan zorgde een zeebeving in 2011 voor een tsunami die ruim 400 m^2 land overspoelde. Miljoenen huishoudens kwamen zonder drinkwater of elektriciteit te zitten, en een kernramp kon ternauwernood worden voorkomen. De reguliere

telecommunicatielijnen (over land en mobiel) vielen uit, waardoor al het contact tussen mensen en hulpdiensten onderling via internet moest gebeuren[49]. Keteneffecten kunnen er dus voor zorgen dat dreiging binnen de ene categorie dreiging binnen een andere categorie veroorzaakt.

Naast dynamische veranderingen en keteneffecten ten gevolge van samenhang, wordt de dreigingsrealiteit in steeds grotere mate door een derde ontwikkeling gecompliceerd: de verweving van interne en externe veiligheid. In de strategische monitor van 2014 (Rood, 2014, p.130), van het Instituut Clingendael staat het volgende:

> *"Er is sprake van een paradoxale ommekeer: tijdens de Koude Oorlog was de externe militaire dreiging groot maar het gevaar hiervan voor de interne veiligheid was juist gering door de vastgevroren Oost-West verhouding; thans is de externe militaire dreiging gering maar heeft instabiliteit elders in de wereld wel directe gevolgen voor de interne veiligheid. Illegale immigratie, terrorisme, georganiseerde criminaliteit en cyber zijn hiervan voorbeelden. Deze veiligheidsrisico's zijn niet te bestempelen als 'extern' noch als 'intern'. Ze zijn grensoverschrijdend, niet alleen vanuit nationaal perspectief maar ook op Europees niveau. Verwevenheid van externe en interne veiligheid is dan ook geen vraag maar realiteit."*

Deze verwevenheid van binnenlandse en buitenlandse veiligheidsvraagstukken wordt onderschreven door de WRR (2017a, p.41):

> *"Veiligheid en onveiligheid manifesteren zich meer dan voorheen in netwerken die zich niet laten indelen in 'intern' en 'extern'. Het internationale terrorisme getuigt daarvan, evenals de – nog steeds onvoldoende afgeremde – internationale wapenhandel. Onbeheerste interne conflicten zoals die in Oekraïne en Syrië kregen een enorme grensoverschrijdende impact, in het ene geval in de vorm van politieke en militaire interventies door een buurland, in het andere geval door het vertrek van grote aantallen vluchtelingen naar andere landen in het Nabije Oosten en Europa. Ook de internationale risico's als gevolg van Da'esh zijn voortgekomen uit onverzoenlijke tegenstellingen in Irak en de Levant."*

Naast deze vervlechting van in- en externe veiligheidsaangelegenheden, constateert de WRR bovendien dat de aard van dreigingen is veranderd en dat dit een verslechterde veiligheid voor Nederland tot gevolg heeft. Immers, de verschuiving van een unipolaire naar een multipolaire wereldorde, en de daardoor toenemende economische en politieke invloed van onder andere Rusland en China zorgt voor spanningen, rivaliteit, en uitbreiding van de militaire macht. Hierbij is Nederland direct betrokken. Digitaliteit, de bedreigingen van vitale infrastructuren en de inzet van desinformatie zetten de toon ten aanzien van deze hernieuwde dreigingen. Men illustreert (WRR, 2017, p.20):

> *"Het neerschieten van vlucht MH17 boven Oekraïens grondgebied, vluchtelingenstromen uit Syrië en andere landen, de strijd met Da'esh in Syrië en Irak, en terroristische dreigingen maken duidelijk dat veel brandhaarden in de wereld directe of indirecte impact hebben op Nederland. Conflicten in het buitenland werken in eigen land door, zoals spanningen tussen bevolkingsgroepen en botsingen over de Gülenscholen na de mislukte putsch in Turkije van 15 juli 2016 en over het Turkse constitutionele referendum."*

Dit alles leidt de WRR ertoe te constateren dat het onderscheid tussen intern en extern, tussen dreigingen voor de openbare orde en buitenlandse veiligheidsvraagstukken, achterhaald is en geen recht doet aan de realiteit. Men doet twaalf aanbevelingen aan de overheid, waarvan de eerste twee in deze context boekdelen spreken, namelijk tot versterking van de verbinding tussen intern en extern veiligheidsbeleid, en het samenvoegen van de twee veiligheidsstrategieën (Strategie Nationale Veiligheid en Internationale Veiligheidsstrategie).

[49] zie bijvoorbeeld https://www.volkskrant.nl/nieuws-achtergrond/zeewater-om-kernsmelting-te-voorkomen~b6ed37a5/

Het kabinet geeft in diens reactie op het WRR-rapport[50] aan de bevindingen ten aanzien van de verweving van in- en externe veiligheid te onderschrijven, evenals de verslechterde Nederlandse veiligheidspositie. Het stelt overeenkomstig de aanbevelingen de Geïntegreerde Buitenland- en Veiligheidsstrategie te hebben opgesteld, evenals de Defensienota. Bovendien verwijst men naar de inmiddels daadwerkelijk gepubliceerde Nationale Veiligheid Strategie 2019 (NCTV, 2019b), waarin vanuit de vervlechting van intern en extern naar veiligheidsvraagstukken wordt gekeken. Opvallend is de volgende passage uit de kabinetsreactie (p.5), waarin men ook op organisationeel toenadering tussen de traditionele veiligheidsapparaten, verantwoordelijk voor de interne en externe veiligheid, aankondigt:

> *"Het bevorderen van de maatschappelijke inbedding van de krijgsmacht door civiel-militaire samenwerking vormt een gedeelde verantwoordelijkheid van alle betrokken departementen. Deze kunnen hieraan alleen in samenwerking met maatschappelijke organisaties, kennisinstellingen en bedrijfsleven op een volwaardige manier gestalte geven. Defensie heeft de afgelopen jaren een voortrekkersrol gespeeld in de oprichting van baanbrekende vormen van samenwerking met internationale partners, waaronder pooling and sharing van capaciteiten. Ter versterking van een robuuste en wendbare krijgsmacht zal de komende tijd ook de samenwerking met civiele partners verder worden verdiept."*

En, iets verderop:

> *"Waar mogelijk is de Nederlandse bijdrage onderdeel van een geïntegreerde benadering, waarbij civiele inzet naast de diplomatieke, ontwikkelingssamenwerking en militaire middelen, onontbeerlijk is."*

Niet enkel verandering in het dreigingsbeeld, maar ook de reactie op die verandering laat dus een vervlechting van intern en extern zien. Klaarblijkelijk zijn samenwerking, integraliteit en gedeelde verantwoordelijkheid dé manier om vorm te geven aan de vernieuwde veiligheidszorg. Om praktische vorm te geven aan deze woorden, wordt in de Nationale Veiligheid Strategie 2019 gesteld dat een drietal publicaties dient om de aanpak uit te leggen: de Nationale Veiligheid Strategie 2019 (NVS); de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS); en de Defensienota. Hierbij wordt de reactie op de verwevenheid van intern en extern, en de noodzaak tot een geïntegreerde aanpak van nationale veiligheid vooral besproken in de NVS, die eerdere analyses zoals het Dreigingsbeeld Terrorisme Nederland, de Strategische Monitor en het NVP integreert. De NVS beschrijft nog steeds verschillende dreigingscategorieën (zoals inmenging van statelijke actoren; terrorisme en extremisme; verstoring van vitale infrastructuur; militaire dreigingen; criminele ondermijning; cyberdreigingen; en natuurrampen), maar heeft vooral ook aandacht voor de bovenliggende macrotrends en -ontwikkelingen die het dreigingsbeeld beïnvloeden, zoals internationale (politieke) ontwikkelingen; technologische ontwikkelingen; mondiale financieel-economische ontwikkelingen; demografische en maatschappelijke ontwikkelingen; en ecologische ontwikkelingen.

De verwevenheid van interne en externe veiligheid vraagt volgens de NVS om meer integratie van de nationale veiligheidsaanpak. Hierbij wordt ingezet op een maatschappijbrede aanpak waarbij overheidsorganisaties, veiligheidsdiensten, het bedrijfsleven en burgers een belangrijke rol hebben. Veiligheid mag dan een kerntaak van de overheid zijn, deze overheid kan deze echter niet (meer) alléén realiseren (NCTV, 2019b).

[50] zie https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2018Z05555&did=2018D21987

4.2 Digitalisering als oorzaak én als aparte categorie

De vorige paragraaf liet zien dat megatrends en -ontwikkelingen ervoor gezorgd hebben dat onderscheiden tussen dreigingen voor de interne en externe orde vervagen. Één van deze macro-ontwikkelingen betreft digitalisering.

Steeds meer facetten van ons maatschappelijk leven en handelingen waarvan we als maatschappij vinden dat deze ongestoord doorgang zouden moeten kunnen vinden spelen zich niet enkel in de fysieke, maar (ook) in de digitale sfeer (*cyberspace*) af (Bantema et al., 2018). Dit leidt er onvermijdelijk toe dat potentiële dreigingen voor het maatschappelijk leven steeds vaker ook een digitale variant of component kennen (Anderson et al., 2014). Digitalisering levert welvaart, vrijheid en gebruiksgemak, en in veel situaties bovendien verhoogde veiligheid. Met de verhuizing of uitbreiding van fysieke zaken als communicatie, betalingen, beveiliging, overheidsdiensten en vitale infrastructuur naar de digitale sfeer volgen echter ook potentiële dreigingen hiervoor naar cyberspace (Brenner, 2014). Zo is een situatie ontstaan waarin potentiële dreigingen en diens gevolgen in meer of mindere mate gedigitaliseerd zijn. Dreigingen in de fysieke (kinetische) wereld bestaan vanzelfsprekend nog steeds, evenals de fysieke gevolgen die deze dreigingen kunnen veroorzaken. Momenteel zijn er echter ook compleet digitale dreigingen denkbaar, met puur digitale (maar zeer schadelijke) gevolgen. Ook beide tussenvormen zijn mogelijk: digitale dreigingen met vooral fysieke gevolgen; of fysieke dreigingen waarvan de gevolgen zich vooral in de digitale sfeer voltrekken. Met betrekking tot deze laatste twee gevallen wordt ook wel gesproken van 'hybride' dreigingen: mengelingen van conventionele en onconventionele dreigingen (Cusumano & Corbe, 2018; NCTV, 2016).

Brenner (2014) stelt dat *'cyberspace'* een nieuwe variabele in de definitie van dreigingen en controle creëert. Activiteiten kunnen nu via een relatief nieuwe, niet-fysieke dimensie worden verricht. Dit is ook het beeld dat geschetst wordt in de NVS: systemen en apparaten die eerder enkel voorgeprogrammeerde handelingen konden verrichten volgens strakke protocollen, zijn in steeds hogere mate zelflerend en autonoom. Bovendien zijn steeds meer apparaten (van huishoudelijke apparaten tot bruggen en sluizen) verbonden met het internet. Daarnaast is de maatschappij in grote mate afhankelijk geworden van technologieën die in veel gevallen door buitenlandse techbedrijven gemaakt en onderhouden worden. Ten slotte zorgt de opkomst van cryptovaluta en *blockchain*technieken voor grote veranderingen in de financieel-economische sector. Digitalisering als macrotrend betreft dus niet enkel het wereldwijd verplaatsen van activiteiten van het fysieke naar het digitale domein; het betreft ook wereldwijde vernetwerking en verknopen, en handelingen en activiteiten die wereldwijd exclusief in het digitale domein worden verricht.

Digitalisering is een van de macrotrends die als aanjagende factoren zorgen voor de verweving van interne en externe veiligheidsaangelegenheden, door de genoemde vernetwerking en internationale afhankelijkheden. Brenner (2014) legt dit uit door te stellen dat oorlogshandelingen eerder nog dreigingen waren die enkel van andere natiestaten af konden komen, en (terroristische) misdaden en overtredingen enkel daden van burgers uit binnen- of buitenland. Deze onderscheiden vervagen; staten kunnen via digitale kanalen *ook* criminele activiteiten ontplooien, en burgers en bedrijven kunnen *ook* oorlogshandelingen verrichten, zonder zelf fysiek in de buurt te zijn van de getroffenen. Ter illustratie: analisten claimen dat China voor digitale oorlogspraktijken burgergroeperingen inzet, samen met (semi-) professionele staatsgelieerde officials[51]. Hierdoor zijn dreigingen volgens het CSBN 2018[52] vaak

[51] zie bijvoorbeeld http://content.time.com/time/world/article/0,8599,1940009,00.html

[52] zie https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf

ook niet meer in een vroeg stadium te classificeren als interne of externe dreiging; als bedreiging voor de nationale veiligheid of voor de openbare orde; als zaak voor de krijgsmacht of als zaak voor de politie[53].

Digitalisering is bovendien ook een van de onderdelen van het geheel aan dominante risico's dat momenteel het dreigingsbeeld bepaalt: de digitale dreiging is volgens het Cyber Security Beeld Nederland (CSBN) 2019[54] permanent. 'Cyberdreigingen' betreffen onder meer spionage; informatie- en systeemmanipulatie; verstoringen; informatiediefstal; storing/uitval; en datalekken. Staten en criminelen vormen daarbij de grootste dreiging. Het CSBN 2018[55] laat zien dat de ene 'combinatie' van actor, dreiging en doelwit waarschijnlijker en/of ernstiger is dan de andere, maar dat 'cyberspace' voorheen 'onmogelijke' combinaties mogelijk maakt: burgers en bedrijven kunnen getroffen worden door de digitale activiteiten van staten (en andersom). Attributie van digitale aanvallen is bovendien een zeer complexe aangelegenheid; het vereist technisch hoogwaardige capaciteiten, waarvan bekend is dat slechts enkele staten deze bezitten. Het risico bestaat hiermee dat bedrijven, burgers en overheidsorganisaties aanvallen niet kunnen toewijzen, of dit zelfs foutief doen (NCTV, 2018b).

De verplaatsing van traditionele dreigingen van het fysieke naar het digitale domein, en de ontwikkeling van nieuwe dreigingen aldaar, zijn voer voor journalisten en wetenschappers om zich te richten op zaken als cyberoorlogen[56], cyberterrorisme en cybercrime. Hoewel veel publicaties waarschuwen voor de potentiële gevaren van digitale oorlogsvoering en digitaal terrorisme, wijzen anderen op het feit dat (mede afhankelijk van definities) daadwerkelijke digitale oorlogsvoering en terrorisme (nog) niet hebben plaatsgevonden. Wetenschappers stellen dat digitale activiteiten eigenlijk niet als oorlogshandelingen aangemerkt kunnen worden vanwege het gebrek aan dodelijke gevolgen, instrumentele karakter en politieke aard. Tot nu heeft geen enkele cyberaanval, groot of klein, op zichzelf de combinatie van deze (aan Clausewitz ontleende) karakteristieken vertoond (Rid, 2012). Alle incidenten tot nu toe kunnen beter geclassificeerd worden als ondermijning, spionage, sabotage of digitale criminaliteit. In de 'Inventarisatie veiligheidstrends'[57] van de Veiligheidscoalitie Midden-Nederland wordt een toename vastgesteld in de mate waarin traditionele criminaliteit verweven raakt met digitale criminaliteit. Voorbeelden hiervan zijn digitale fraude, hacken, illegaal downloaden, aanbieden van illegale prostitutie via internet, digitaal pesten, Ddos- aanvallen en ransomware. Ook een deel van ondermijning vindt digitaal plaats, zoals *darkweb* om wapens en drugs te verhandelen, nepwinkels[58], of bitcoins als crimineel betaalmiddel[59]. Dergelijke criminele activiteiten hebben vanwege hun verplaatsing naar het digitale domein steeds vaker een internationaal karakter, in plaats van nationaal of zelfs lokaal. Dit belemmert de mogelijkheden tot opsporing en aanhouding aanzienlijk (Anderson et al., 2013)

Digitale aanvallen op bedrijven zijn in de periode 2012-2017 verdubbeld[60], en incidenten die voorheen nog als uitzonderlijk konden worden beschouwd zijn inmiddels steeds

[53] dit laatste is een probleem dat niet exclusief is voorbehouden aan digitale dreigingen. Ook op andere - fysieke - gebieden is er sprake van dreigingen waarvan niet duidelijk is onder wiens verantwoordelijkheid deze vallen; denk aan het onderscheppen van drugs door de Amerikaanse krijgsmacht, waardoor deze *de facto* politietaken op zich heeft genomen (Dunlap, 1999).

[54] zie https://www.nctv.nl/binaries/CSBN2019_online_tcm31-392768.pdf

[55] zie https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf

[56] zie bijvoorbeeld https://www.nrc.nl/nieuws/2018/10/14/minister-van-defensie-cyberoorlog-met-rusland-a2510671

[57] zie https://veiligheidscoalitie.nl/action/?action=download&id=1951

[58] zie bijvoorbeeld https://nos.nl/artikel/2292141-politie-pakt-grootste-spaanse-internetoplichter-ooit-op.html

[59] zie bijvoorbeeld https://www.om.nl/actueel/nieuwsberichten/@106456/eis-jarenlange/

[60] zie http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

meer gemeengoed. Belangrijk voorbeelden hiervan zijn de *Wannacry*- en *NotPetya*-aanvallen. Een andere opwaartse trend is het gebruik van cyberaanvallen met vitale infrastructuur en strategische industriële sectoren als doelwit, met zorgen voor worst-case scenario's tot gevolg, waarin aanvallers complete verstoringen veroorzaken in systemen die de maatschappij laten functioneren (World Economic Forum, 2018). Hoewel het World Economic Forum een dergelijke maatschappelijke ontwrichting nog als 'worst case scenario' aanmerkt (en daarmee als erg, maar met zeer geringe waarschijnlijkheid), kopt het CSBN 2019 dat een dergelijke ontwrichting van de samenleving 'op de loer' ligt vanwege de afhankelijkheid van een groot aantal (ook vitale) systemen van een beperkt aantal aanbieders; de laagdrempelige toegankelijkheid van aanvalscapaciteiten; achterblijvende weerbaarheid; en doorgroeiende dreiging vanwege alsmaar verdergaande digitalisering.

4.2.1 Deelconclusie: beantwoording deelvraag 3

De derde deelvraag die in dit onderzoek aan de orde is, 'Wat zijn digitale dreigingen en hoe veranderen deze het algemene dreigingsbeeld?', kan op basis van de in dit hoofdstuk besproken bevindingen beantwoord worden. Digitale dreigingen zijn

- ontwikkelingen, handelingen of gebeurtenissen,
- die zich op enige wijze voltrekken via of met behulp van digitale technologieën,
- en de nationale veiligheidsbelangen zodanig in gevaar brengen dat sprake is van (potentiële) maatschappelijke ontwrichting.

Digitalisering is bovendien enerzijds een van de oorzaken van een dynamisch, veranderend dreigingsbeeld. Het zorgt, samen met andere macrotrends, voor vervlechting van interne en externe veiligheid en voor steeds verdergaande samenhang tussen verschillende dreigingscategorieën ten gevolge van vernetwerking. Anderzijds betreft het een dreigingscategorie op zich, waarbinnen een veelheid aan actoren via een veelheid aan kanalen een veelheid aan doelwitten kan treffen.

HOOFDSTUK VIJF
PLURALISERING IN DE VEILIGHEIDSZORG

In het vorige hoofdstuk is de derde van de vijf deelvragen van dit onderzoek beantwoord. In dit hoofdstuk vindt beantwoording van de vierde, naar case gesplitste deelvraag plaats. Zoals reeds besproken is, zorgt digitalisering als één van de huidige 'macrotrends' voor de vervaging van de splitsing tussen interne en externe veiligheid. Dit werpt de vraag op wat dat betekent voor de traditionele instituties, waarvan de taken en verantwoordelijkheden oorspronkelijk juist gebaseerd zijn op deze splitsing. Leidt de verandering van het dreigingsbeeld ten gevolge van de technologische en maatschappelijke ontwikkelingen die digitalisering veroorzaakt tot veranderingen voor de traditionele veiligheidsapparaten, en voor de rollen die bedrijven en burgers spelen in de totstandkoming van veiligheidszorg?

Middels het in hoofdstuk 2 en 3 besproken beoordelingskader wordt hier geanalyseerd in welke mate er sprake is van (de-)centralisatie bij de krijgs- en politionele macht. Bovendien worden de voorschriften aan, en het daadwerkelijke gedrag van, bedrijven en burgers geanalyseerd om zo hun rollen en verantwoordelijkheden in de totstandkoming van veiligheidszorg ten aanzien van digitalisering inzichtelijk te maken. Ten aanzien van alle cases wordt ook rekening gehouden met de maatschappelijke en organisationele context waarin zij zich bevinden, en de bredere bestuurlijke paradigmaverschuiving van de klassieke manier van besturen, via NPM, naar NPG. Immers, om recht te doen aan de complexiteit die de verschillende besproken macrotrends met zich meebrengen, kunnen de manieren waarop de cases omgaan met digitalisering niet 'verkokerd' gezien worden, los van hun bredere context.

5.1 Politionele macht: veranderende dreiging, veranderend bestuur en centralisatie

Middels de Politiewet 2012[61] zijn de 25 regiokorpsen en het Korps landelijke politiediensten KLPD vervangen door tien regionale en één nationale eenheid van huidige Nationale Politie (Jansen, 2016). Deze reorganisatie vond plaats vanwege een verscheidenheid aan redenen. Ten eerste was één nationaal korps noodzakelijk om zware en georganiseerde criminaliteit, cybercriminaliteit, en terrorisme te kunnen bestrijden (Koopman, 2013). Nieuwe vormen van sociale onveiligheid, zoals georganiseerde misdaad, organisatiecriminaliteit, cybercrime of terrorisme, kenmerken zich erdoor dat zij niet aan één (vaste) locatie zijn gebonden (Terpstra & Van der Vijver, 2005). Tot die tijd ondermijnde de versnippering de slagkracht van de politie. Korpsen werkten niet of nauwelijks samen, waardoor criminelen die in meerdere regio's of andere landen opereerden de dans konden ontspringen[62]. Men stelde dat de 'eigenlijke taak' van de politie (handhaving en opsporing (Van der Vijver et al., 2001)) in een tijdvak van internationale criminaliteit en terrorisme niet meer te realiseren was met een gefragmenteerd en gedecentraliseerd politiebestel. Samen met kritiek vanuit het buitenland op de wijze waarop de politie in Nederland omging met internationale rechtshulpverzoeken, is zo een druk ontstaan om meer aandacht te geven aan de 'harde' kant van de politie en deze meer op een centraal niveau te organiseren (Terpstra & Van der Vijver, 2005).

Ten tweede was vóór de inwerktreding van de Politiewet 2012 het beheer over de regiokorpsen in handen van de regionale korpsbeheerders (meestal de burgemeester van de

[61] zie https://wetten.overheid.nl/BWBR0031788/2019-02-01#Hoofdstuk1

[62] zie https://decorrespondent.nl/2891/waarom-moest-de-nationale-politie-er-ook-alweer-komen/984621671572-110cfb0a

grootste regiogemeente). Deze maakte keuzes voor onder meer eigen ICT-systemen, de inkoop van materieel en personeelsbeleid, wat zorgde voor inefficiëntie en slechte samenwerkingsmogelijkheden (KPMG, 2009).

Om de problemen omtrent efficiëntie en samenwerkingsmogelijkheden op te kunnen lossen, stelde KPMG (2009) in diens *Feasibility Studies naar de PIOFACH[63] taken van de politie (deel 1)* voor om het beheer over de korpsen op een andere manier te organiseren. De verwachting was dat dit een grote verbetering zou betekenen voor de kwaliteit, effectiviteit en efficiëntie van de bedrijfsvoeringsprocessen. Die verbetering waren langs drie lijnen mogelijk:

- landelijke kaderstelling en beperking van maatwerk, daar waar standaard ook volstaat;
- standaardiseren en automatiseren van werkprocessen;
- concentreren van uitvoering van werkzaamheden, daar waar schaalvoordelen en kwaliteitsverbetering gerealiseerd kunnen worden.

Om tot dergelijke verbeteringen te komen werd onder meer onderbrenging van het beheer over de korpsen, landelijke aansturing van processen en concentratie van medewerkers geadviseerd (KPMG, 2009). De inefficiëntie en beperkte samenwerkingsmogelijkheden (zoals het gebruik van verschillende ICT-systemen door verschillende korpsen, waardoor onderlinge communicatie bemoeilijkt was) leidden tot moeilijkheden in de aansluiting bij de hierboven besproken (schaal-) veranderingen in misdaad en criminaliteit.

Ten derde is in de jaren voorafgaand aan de reorganisatie van 2012, in nauwe samenhang met de beheersmatige overwegingen, het voor NPM karakteristieke bedrijfsmatige denken de boventoon gaan voeren in bestuurlijke keuzes, ook ten aanzien van de politie: de invoer van prestatiecontracten; de karakterisering van burgers als 'klant' van de politie; onvrede over regiokorpsen die teveel 'hun eigen gang gaan'; en het idee dat criminaliteitsbestrijding duidelijke en meetbare output heeft (Terpstra & Van der Vijver, 2005).

De Politiewet van 2012 heeft op een aantal manieren gezorgd voor organisationele centralisatie, waarvan de volgende conclusies getuigen:

- De Minister van Justitie en Veiligheid is verantwoordelijk voor de begroting van de Nationale Politie, en voor de manier waarop middelen over eenheden worden verdeeld[64];
- De relatieve autonomie van decentrale actoren is met deze reorganisatie nog verder afgenomen dan bij de eerdere politiewetten ook al het geval was, ten gunste van de controle die het Ministerie van Justitie en Veiligheid nu als centraal bestuursorgaan over de organisatie kan uitvoeren. Decentrale actoren, zoals burgemeesters, ervaren dit zelf in de praktijk ook als zodanig (Terpstra et al., 2015);
- De Minister van Justitie en Veiligheid stelt elke vier jaar voor de landelijke en regionale eenheden de doelstellingen ter verwezenlijking van de landelijke beleidsdoelen vast[65];
- Toezicht op de Nationale Politie ligt belegd bij de Inspectie Openbare Orde en Veiligheid, die onder direct gezag van de Minister van Justitie en Veiligheid staat[66];

Er is echter niet alleen maar sprake van centralisatie. Er is immers ook een trend van *pluralisering* gaande, wat decentralisatie van taken inhoudt die niet meer als kerntaken worden aangemerkt. Verschillende vormen van openbare ordeverstoringen zorgen immers voor betrokkenheid van steeds verschillende instanties en overheden (zoals milieudiensten, GGD,

[63] PIOFACH: Personeel, IT, Organisatie, Financiën, Inkoop, Huisvesting en Communicatie

[64] zie https://wetten.overheid.nl/BWBR0031788/2019-02-01#Hoofdstuk3_Afdeling3.2_Paragraaf3.2.3_Artikel34

[65] zie artikel 20 van de Politiewet 2012

[66] zie https://wetten.overheid.nl/BWBR0031788/2019-02-01#Hoofdstuk6

private organisaties, provincie, het Rijk) (Instituut Fysieke Veiligheid, 2018). Dit leidt politieonderzoekers ertoe te stellen dat ook de politie zich dient op te stellen als speler in een netwerk. De Nationale Politie lijkt zich daarbij meer op 'spannende' kerntaken te richten, terwijl decentrale diensten als boa's, gemeentelijke toezichthouders, stadswachten en handhavers meer en meer verantwoordelijk worden voor contact met burgers en handhaving van de openbare orde. Deze lokale toezichthouders krijgen stukje bij beetje een steeds uitgebreider takenpakket, verdergaande bevoegdheden en dwangmiddelen, al stuit dit laatste ook op verzet[67]. Dit leidt tot een 'duaal bestel' met betrekking tot politiewerk (Terpstra & Van Stokkom, 2015): er is in Nederland dus sprake van één gecentraliseerd traditioneel politiekorps, maar een politielandschap dat uit een grote hoeveelheid aan actoren bestaat, waarvan een aantal vooral decentraal acteert. Bovendien klinkt de laatste jaren (conform de algehele bestuurlijke NPG-ontwikkeling) de roep om meer decentraliteit, onder meer door een grotere mate van autonomie te beleggen bij decentrale actoren als eenheidschefs; vertrouwen te hebben in hun professionaliteit; en ruimte te bieden voor lokaal maatwerk[68]. Dit wordt erkend door de minister; hij stelt middels minder strakke sturing decentrale actoren meer ruimte te willen geven om operationeel en beheersmatig gevolg te kunnen geven aan de prioriteiten van het lokaal gezag[69].

Een veranderend dreigingsbeeld en het verschuivende bestuurlijk paradigma zijn dus de hoofdzakelijke factoren die hebben geleid tot de invoering van de Politiewet 2012. Met deze wet is steeds meer centralisatie in de organisatie van de politionele macht gekomen (Koopman, 2013), maar conform het veranderende bestuurlijke paradigma worden nu ook alternatieven voor deze strakke sturing van bovenaf gezocht. De digitalisering van dreigingen is onderdeel van het veranderende dreigingsbeeld, en is als zodanig (algemeen gezien) mede aanjager van de organisationele centralisatie. Digitalisering is echter niet de enige veranderende factor. De vraag is nu welke specifieke maatregelen er door en ten aanzien van de politionele macht zijn genomen, die betrekking hebben op de omgang met de digitalisering van dreigingen. Immers, mogelijkerwijs spreekt ook uit deze praktische maatregelen een bepaalde mate van (de-) centralisatie.

5.1.1 Maatregelen ten aanzien van digitalisering van dreigingen

Maatregelen ten aanzien van de politionele macht, met betrekking op de digitalisering van dreigingen, zijn zonder uitzondering onderdeel van bredere pakketten aan maatregelen om "alle partijen die een deelverantwoordelijkheid hebben in preventie, pro-actie, preparatie, respons en nazorg" samen te laten werken (NCTV, 2019b, p.12). 'Integraliteit' is daarbij het toverwoord. Maatregelen zijn vooral gefocust op het verhogen van *weerbaarheid*, en behelzen onder andere:

- De oprichting van een cybersecurity-alliantie om publieke en private partijen te verbinden, en zo de maatregelen uit de Nederlandse Cyber Security Agenda[70] vorm te geven. De politie is onderdeel van deze alliantie;
- Het Team High Tech Crime (THTC) van de politie is sinds 2012 fors uitgebreid[71];

[67] zie bijvoorbeeld https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/g40-laat-keuze-bewapening-boa-s-aan-driehoek.9603406.lynkx

[68] zie bijvoorbeeld Kuijken et al. (2017).

[69] zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/06/15/kamerbrief-over-de-evaluatie-politiewet-2012/kamerbrief-over-de-evaluatie-politiewet-2012.pdf

[70] zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf

[71] zie bijvoorbeeld https://www.channelweb.nl/artikel/nieuws/security/4684680/5226433/team-high-tech-crime-werft-dertig-rechercheurs.html

- De komende jaren worden ook de regionale cybercrime-teams van de Nationale Politie verder uitgebreid[72] conform het Regeerakkoord[73], waarin een reservering van structureel 95 miljoen euro wordt aangekondigd voor cybersecurity;
- Er wordt meer ingezet op publiek-private samenwerking voor de aanpak van cybercrime, onder meer door verbeterde informatie-uitwisseling. Ook worden een expertisecentrum digitale opsporing en een kennis- en expertisecentrum cybercrime ingericht[74];
- De Nederlandse Cyber Security Agenda (NCSA) bespreekt ten slotte een veelheid aan te nemen maatregelen om veiligheid in het digitale domein te garanderen, waarbij containerbegrippen als publiek-private samenwerking; cross-sectoraliteit; integraliteit; en informatiedeling talrijk zijn. Zelden worden daarbij specifieke taken gespecificeerd, ook niet voor de politionele macht. Het zal echter weinig controversieel zijn aan te nemen dat van de politie ook verwacht wordt zich volgens de in de NCSA gestelde kaders op te stellen.

5.1.2 Fiscale, Politieke en Bestuurlijke (de-)centralisatie?

Deze thesis heeft zichzelf ten doel gesteld middels een beoordelingskader te bepalen of er bij de krijgs- en politionele macht sprake is van centralisatie of decentralisatie, *ten aanzien van de digitalisering van dreigingen*. Het is echter duidelijk geworden dat de reorganisatie van de politionele macht een reactie was op een *scala aan overwegingen en blootgelegde problemen* ten gevolge van brede maatschappelijke en bestuurlijke ontwikkelingen. Bovendien is de politionele macht lang niet meer de enige actor die zich bezighoudt met politiewerk. De waargenomen pluralisering compliceert de mogelijkheden om het beoordelingskader toe te passen. Immers, samen vormt het gefragmenteerde netwerk aan actoren die politiewerk verrichten geen organisatie waarbinnen een duidelijke fiscale, politieke en bestuurlijke lijn te herkennen valt. De maatregelen die de overheidsorganisaties nemen om sturing te geven aan de samenwerkingsverbanden binnen het netwerk, passen binnen de algemene bestuurlijke NPG-trend waarin de overheid optreedt als netwerkpartner: meerdere wederzijds afhankelijke actoren opereren in het netwerk om zo samen bij te dragen aan de levering van publieke diensten, in dit geval politiewerk (zie ook §2.1.4).

De fiscale, politieke en bestuurlijke indicatoren van het 'politiewerk-netwerk' wijzen simpel gezegd op decentralisatie. Immers, het netwerk wordt geconstitueerd door een heterogene populatie aan publieke en private actoren; het zijn organisaties op zich[75]. Deze netwerkpartners gaan over het algemeen over hun eigen financiën, beschikken binnen de kaders van samenwerking over een grote mate van autonomie en medezeggenschap, en kennen een hoge mate van street-level-bureaucracy. Dergelijke netwerken opereren doorgaans los van hiërarchische centrale overheidsstructuren (Osborne, 2006).

De organisatie van de Nationale Politie zelf kan wél min of meer middels het beoordelingskader getoetst worden op fiscale, politieke en bestuurlijke (de-)centraliteit. Door dat te doen blijkt een hoge mate van centraliteit *binnen* deze organisatie. Immers: de Minister

[72] zie bijvoorbeeld https://www.agconnect.nl/artikel/politie-wil-regionale-cybercrimeteams-vergroten

[73] zie https://www.kabinetsformatie2017.nl/binaries/kabinetsformatie/documenten/publicaties/2017/10/10/regeerakkoord-vertrouwen-in-de-toekomst/Regeerakkoord+2017-2021.pdf

[74] zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/begrotingen/2018/09/18/begroting-nationale-politie-2019/Begroting-Beheerplan+Nationale+Politie+2019-2023.pdf

[75] zie bijvoorbeeld https://www.computable.nl/artikel/nieuws/security/6366295/250449/grapperhaus-geeft-starschot-cybersecurity-alliantie.html en https://www.alertonline.nl/overzicht-partners

van Justitie en Veiligheid gaat over de begroting en de verdeling van middelen; de korpschef en leidinggevende van landelijke en regionale eenheden worden bij ministeriële regeling aangewezen[76]; decentraal beleid wordt aan centrale doelstellingen aangepast; en de mate waarin decentrale autonomie en street-level bureaucracy mogelijk is, is sterk gedaald (Terspstra & Gunther Moor, 2012; Kuijken et al., 2017). Vanzelfsprekend kan het ministerie niet tot in detail voorkomen dat er regionale verschillen bestaan in de taakuitvoering van de Nationale Politie[77], maar vergeleken met de situatie vóór de invoering van de Politiewet 2012 is in de organisatie van de politionele macht een sterke mate van centralisatie op alle indicatoren vast te stellen. Deze centralisatie valt echter niet in isolatie te wijten aan de digitalisering van dreigingen. Andere overwegingen hebben een belangrijker aandeel gehad in de organisationele centralisatie bij de politionele macht. Puur kijkend naar digitalisering, dan kan geconcludeerd worden dat deze juist geleid heeft tot pluralisering, versnippering en, daarmee, decentralisatie van politiewerk.

5.1.3 Deelconclusie: beantwoording deelvraag 4a

Het eerste deel van de vierde deelvraag in deze thesis is 'wat zijn de gevolgen van digitale dreigingen voor de organisatie, taken en verantwoordelijkheden van de politionele macht?'. Op basis van bovenstaande analyse kan geconcludeerd worden dat de politionele macht in Nederland, om digitale dreigingen te mitigeren, zich in toenemende mate als netwerkpartner in publiek-private samenwerkingsverbanden opstelt. De sterke centralisatie die die Politiewet 2012 tot gevolg had, kan niet of nauwelijks geïsoleerd worden toegeschreven aan de digitalisering van dreigingen omdat deze een reactie was op enkele grote veranderingen op maatschappelijk en bestuurlijk vlak. Bovendien is digitalisering één van de veranderingen waaraan dreigingen onderhevig zijn, naast bijvoorbeeld internationalisering[78]. Digitalisering van dreigingen heeft wél tot gevolg gehad dat naast de Nationale Politie een veelheid aan andere actoren betrokken is geraakt bij het verrichten van politiewerk. Politiewerk ten aanzien van de digitalisering van dreigingen heeft daarmee een gepluraliseerd karakter gekregen, en het totale netwerk aan actoren dat de verantwoordelijkheid voor dit politiewerk op zich neemt, is sterk decentraal van aard. Overheidsinstellingen fungeren binnen dit netwerk als partner en facilitator, passend bij de algehele huidige bestuurlijke trend.

5.2 Krijgsmacht: investeren na bezuiniging, autonomie en samenwerking

Voor het eerste sinds lange tijd werden er in 2017 investeringen in plaats van bezuinigingen ten aanzien van de krijgsmacht aangekondigd. Het regeerakkoord van kabinet Rutte III laat voor Defensie een budgetverhoging zien naar ruim 1,5 miljard euro per jaar[79]. Uitdrukkelijk wordt erbij vermeld dat er wordt geïnvesteerd in een forse uitbreiding van de cybercapaciteit en technologie bij alle krijgsmachtonderdelen, en dat de digitale beveiliging en bewaking van Nederland wordt versterkt.

Vanaf de jaren '90 heeft de krijgsmacht, ingegeven door de veranderingen in de machtsverhoudingen op het wereldtoneel, in steeds verder afgeslankte vorm moeten opereren (WRR, 2017a). De bezuinigingen op de krijgsmacht waren vooral gelegen in de positieve

[76] zie zie https://wetten.overheid.nl/BWBR0036705/2017-11-29#Hoofdstuk2

[77] zie bijvoorbeeld https://www.ed.nl/brabant/crimineel-is-in-de-ene-brabantse-gemeente-beter-af-dan-in-de-andere~adf5b114/?

[78] vanzelfsprekend houden digitalisering en internationalisering ook weer verband met elkaar.

[79] zie https://www.kabinetsformatie2017.nl/binaries/kabinetsformatie/documenten/publicaties/2017/10/10/regeerakkoord-vertrouwen-in-de-toekomst/Regeerakkoord+2017-2021.pdf

veranderingen in het dreigingsbeeld na het einde van de Koude Oorlog. Naast dat er steeds minder financiële middelen beschikbaar werden gesteld, dienden er reorganisaties plaats te vinden om de krijgsmacht efficiënter en centraler te laten functioneren[80]. Hoewel er geen sprake was van volledige centralisatie (kleinere projecten konden door de verschillende krijgsmachtonderdelen wel degelijk zelf worden uitgevoerd)[81], ervoeren commandanten steeds minder bevoegdheden, middelen en instrumenten te hebben om de gewenste effectiviteit te bereiken (Van den Berg et al., 2017). Men kon zeer beperkt schuiven met middelen ten tijde van krapte. Zo kregen bijvoorbeeld landmacht, luchtmacht en marine een numerus fixus mee vanuit Den Haag voor alle rangen, en op basis daarvan kregen ze geld[82]. De bezuinigingsrondes hebben ertoe geleid dat de krijgsmacht werd omgevormd tot een 'expeditionaire crisis-respons organisatie[83]' (De Waard, 2011). Wat in verhouding tot deze versobering opvallend is, is de oprichting van het Nederlandse cybercommando DCC, in media ook weleens het 'cyberleger' genoemd[84], in 2014. Er werden in een tijd van bezuinigingen miljoenen in geïnvesteerd om zo 'cyber' tot een vijfde militair domein te maken (naast land, lucht, zee en ruimte). Echter, waar aanvankelijk de bedoeling was om naast defensieve ook indrukwekkende offensieve capaciteiten op te bouwen, gaf toenmalig commandant Boekholdt-O'Sullivan aan dat het DCC in de praktijk vooral fungeerde als verlener van bijstand aan inlichtingendiensten en andere defensieonderdelen. Overigens is de leiding over het DCC centraal belegd; het valt direct onder de Commandant der Strijdkrachten[85].

In 2015 betoogden 38 prominenten dat de bezuinigingen op Defensie te ver waren doorgeschoten[86], en dat het budget voor Defensie met tenminste 1,5 miljard euro diende te worden verhoogd. In 2016 waarschuwde De Algemene Rekenkamer dat ook in aangepaste vorm de krijgsmacht ten gevolge van de vele bezuinigingsrondes niet meer kon voldoen aan de eisen van de minister met betrekking tot diens inzetbaarheid[87]. De WRR (2017a) haalt deze conclusie aan, om vervolgens aan te bevelen over te gaan tot investeringen in een sterkere krijgsmacht, in reactie op de eerder besproken verslechterde veiligheidssituatie waarin Nederland zich bevindt. Een dergelijk advies is in 2017 ook door de AIV gedaan[88].

In diens reactie op het WRR-rapport laat het kabinet bij monde van de Minister van Defensie weten dat de bezuinigingen ten einde zijn, en dat jaarlijks dus een bedrag tot anderhalf miljard euro in Defensie geïnvesteerd zal worden. Bovendien spreekt zij de wens uit om binnen tien jaar op de door de NAVO gestelde norm van een defensiebudget van twee procent van het BBP te zitten[89]. De extra investeringen zijn dus een direct gevolg van de huidige, verslechterde veiligheidssituatie. De Defensienota 2018 beschrijft de manieren waarop deze investeringen

[80] zie https://www.trouw.nl/nieuws/defensie-moet-efficienter-door-dure-europese-plannen~b0eb21334/

[81] zie https://www.ftm.nl/artikelen/reorganisaties-braken-slagkracht-defensie?share=1

[82] zie https://www.groene.nl/artikel/de-wasmachine-is-gaan-roesten

[83] zie https://www.defensie.nl/onderwerpen/tijdlijn-militaire-geschiedenis/1990-2001-naar-een-expeditionaire-krijgsmacht

[84] zie bijvoorbeeld https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254

[85] zie https://www.defensie.nl/actueel/nieuws/2018/07/05/bauer-over-cybercommando-militaire-capaciteit-die-aan-belang-wint

[86] zie https://www.nrc.nl/nieuws/2015/04/23/wankele-wereldorde-vergt-leger-met-grotere-slagkra-1487020-a1240301

[87] zie https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2017/05/17/resultaten-verantwoordingsonderzoek-2016-bij-het-ministerie-van-defensie/Resultaten+VO+2016+Ministerie+van+Defensie+%28X%29_WR.pdf

[88] zie https://aiv-advies.nl/download/db5754e7-f54c-4e56-afb5-8b17c768bb0f.pdf

[89] zie https://www.tweedekamer.nl/downloads/document?id=4ffe5516-00a7-41d4-8071-cd9e5796566c&title=Kabinetsreactie%20op%20het%20adviesrapport%20WRR%20%E2%80%98Veiligheid%20in%20een%20wereld%20van%20verbindingen.%20Een%20Strategische%20Visie%20op%20het%20Defensiebeleid%E2%80%99.pdf

besteed worden; op grote lijnen is dat 'in mensen, slagkracht en zichtbaarheid'[90]. Bovendien wil men civiele autoriteiten ondersteunen en voor hen als partner fungeren, evenals voor maatschappelijke organisaties en het bedrijfsleven. Er wordt toegewerkt naar een "krijgsmacht die is opgewassen tegen technologisch hoogwaardige tegenstanders en 'hybride' dreigingen. De (mondiale) maatschappelijke ontwikkelingen waartegen deze organisationele veranderingen afzet, zijn onder meer geopolitieke verschuivingen (waaronder de vernieuwing en versterking van de Russische krijgsmacht); onevenwichtige groei van de wereldbevolking; en digitalisering (met de inzet van nieuwe technologieën voor oorlogsvoering, inmenging, ondermijning en misleiding).

In 2003 werd de verregaande autonomie die de verschillende krijgsmachtdelen kenden drastisch ingeperkt (WRR, 2017). In een themaonderzoek door de Inspecteur-Generaal der Krijgsmacht uit 2017 naar de mogelijkheden tot het uitoefenen van invloed door eenheden en hun commandanten[91] omschrijft een van hen hun toenmalige gevoel van onmacht met het citaat 'Ik moet een hoop, maar mag een beetje'. Om de invloedssfeer van de operationele commandanten te vergroten, wordt in het themaonderzoek geadviseerd om de bevoegdheden, verantwoordelijkheden en zeggenschap van de operationele commandanten te herzien; schaarste met betrekking tot materieel en personeel op te lossen; en communicatie, coördinatie en co-creatie tussen ketenverantwoordelijken en de operationele commandanten te verbeteren en stimuleren. Tegenwoordig gaan commandanten volgens de Defensienota weer meer ruimte krijgen in de uitvoering. In haar *brief aan de Tweede Kamer aangaande de Vaststelling van de begrotingsstaten van Ministerie van Defensie (X) voor het jaar 2019*[92] geeft de minister in reactie op het themarapport aan het advies tot meer decentralisatie te hebben omarmd. Een aantal bevoegdheden heeft zij decentraal belegd, opdat commandanten meer mogelijkheden kregen in het behoud en de werving van personeel. Commandant der Strijdkrachten Rob Bauer voegt daar het volgende aan toe[93]:

> *"Vanuit Den Haag gaan we de commandanten daarvoor meer ruimte geven – bevoegdheden en geld dus. Zodat ze zelf meer kunnen beslissen en de veranderingen daardoor ook sneller zichtbaar en voelbaar worden. Die ruimte moet ook worden doorgegeven aan de leidinggevenden daaronder, zodat die op alle niveaus gewoon de dingen gaan doen zoals we die hebben bedacht en zoals die in de plannen staan."*

Naast het vergroten van autonomie voor meer decentrale actoren, wordt nadrukkelijk de samenwerking met keten- en netwerkpartners gezocht om in te kunnen spelen op de nieuwe macro-ontwikkelingen. Bovendien wordt nauwere samenwerking met andere staten ('strategische partners' zoals België, Denemarken, Noorwegen en Duitsland)[94].

Één van de macro-ontwikkelingen die ook door Defensie met argusogen wordt bekeken, is de verspreiding van nieuwe, digitale technologieën. Digitalisering dient ook hier op een tweetal manier te worden bezien. Enerzijds is het een mondiale technologische ontwikkeling die één van de factoren betreft die het veranderende dreigingsbeeld beïnvloeden. Het is *niet enkel* digitalisering dat heeft geleid tot een verslechterde veiligheidssituatie voor Nederland, en

[90] zie https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2018/03/26/defensienota-2018/210318+Defensienota+definitief.pdf

[91] zie https://www.defensie.nl/binaries/defensie/documenten/rapporten/2017/06/01/themarapport-igk-de-commandant-in-zijn-kracht/170601+themarapport+CIZK+Definitief.pdf

[92] zie https://zoek.officielebekendmakingen.nl/kst-35000-X-140.pdf

[93] zie https://www.defensie.nl/organisatie/bestuursstaf/cds/weblog/2018/het-roer-om

[94] zie https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2018/03/26/defensienota-2018/210318+Defensienota+definitief.pdf

daarmee tot hernieuwde investeringen in de krijgsmacht. De andere macrotrends spelen een minstens zo grote rol, en in combinatie zorgen ze voor een veranderd mondiaal dreigingsbeeld. De NVS stelt dat digitale aanvallen van andere staten vanwege hun waarschijnlijkheid en mogelijke impact de grootste digitale dreiging vormen voor de nationale veiligheid[95].

Anderzijds vormt de verspreiding van nieuwe technologieën die voor oorlogsdoeleinden kunnen worden ingezet een aparte 'tak van sport' voor de krijgsmacht. Dit betreft het domein van AI, (semi-)autonome wapensystemen, digitale spionage, big data analyse en biotechnologie[96]. Dit betreft specifiek de digitalisering van oorlogsvoering, en de opkomst van dergelijke technologische wapens wordt ook wel de derde revolutie in oorlogsvoering genoemd, na de uitvindingen van het buskruit en de atoombom (Slijper et al., 2019a). Dat lijkt op het eerste gezicht een thema dat buiten het bereik van dit onderzoek valt, maar vanwege de grote afhankelijkheid van private partijen (veelal buitenlandse, grote technologiebedrijven) is dit wel degelijk van belang. De WRR (2017) stelt bovendien dat dergelijke technologieën krijgsmachten waarschijnlijk veel voordeel zullen brengen, maar tegelijkertijd onvermijdelijk ook leiden tot meer kwetsbaarheid van samenlevingen, in het bijzonder van vitale infrastructuur. Voor de toekomstbestendigheid van de krijgsmacht is omarming van deze technologie van vitaal belang, of het nu gaat om het afschrikken van (potentiële) tegenstanders, het verkrijgen en behouden van de overhand in (gewapende) conflicten en het zoveel mogelijk verminderen van de eigen kwetsbaarheid (WRR, 2017). De ontwikkeling van nieuwe technologieën gaat in een dermate hoog tempo dat de krijgsmacht zich moet inspannen om bij te blijven. Bovendien worden nieuwe technologieën die niet voor militaire doeleinden zijn ontworpen, daar wél voor gebruikt, tot onvrede van de producenten[97]. Inmiddels wordt er gevreesd dat de strategische strijd om bij te blijven op technologisch gebied is verworden tot een 'technologische wapenwedloop' waarbij gedeeld begrip tussen staten aangaande de risico's en voordelen van dergelijk technologie achterblijft ten opzichte van de ontwikkelingen (Slijper et al., 2019b). Klassieke *prisoners' dilemma*-overwegingen leiden er echter toe dat staten meegaan in de ontwikkelingen, om verlies te vermijden.

Digitale technologieën, producten en diensten die door krijgsmachten worden gebruikt, worden vooral geleverd door grote techbedrijven als Microsoft en Amazon[98], maar ook Apple, Facebook, Baidu en Alibaba[99]. Vaak ontbreken bij de oplevering van dergelijke technologieën clausules die krijgsmachten ervan dienen te weerhouden de technologie voor gewelds- of oorlogsdoeleinden in te zetten. Daarnaast wordt de krijgsmacht door het gebruik van dergelijke technologieën voor het verdedigen van de nationale belangen afhankelijk van buitenlandse bedrijven. Dit betekent dat bedrijven, naast de krijgsmacht, ook een rol hebben in het leveren van veiligheidszorg, en dat er dus ook ten aanzien van het werk dat traditioneel door de krijgsmacht wordt verricht, sprake is van pluralisering. Paragraaf 5.3 gaat verder in op de rollen en verantwoordelijkheden van de private sector.

Voor de ommezwaai ten aanzien van het belang dat er aan de krijgsmacht wordt gehecht is dus de verslechterde veiligheidspositie van Nederland verantwoordelijk. Deze positie wordt door meerdere macrotrends veroorzaakt, waarvan één digitalisering betreft. Zo gesteld kan de

[95] zie https://www.nctv.nl/binaries/Nationale%20Veiligheid%20Strategie%202019_tcm31-393099.pdf

[96] zie https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2018/03/26/defensienota-2018/210318+Defensienota+definitief.pdf

[97] zie bijvoorbeeld https://www.blog.google/technology/ai/ai-principles/

[98] zie bijvoorbeeld https://www.nu.nl/tech/5980273/pax-microsofts-en-amazons-interesse-in-defensie-is-zeer-zorgwekkend.html?redirect=1

[99] zie bijvoorbeeld https://www.paxforpeace.nl/media/files/pax-report-killer-robots-dont-be-evil.pdf

algemene digitaliseringstrend, die leidt tot vergrote afhankelijkheden en toename in het aantal potentieel dreigende actoren, in beperkte mate verantwoordelijk worden gehouden voor de omslag van bezuinigen naar investeren. Overige organisationele veranderingen zoals vergrote autonomie voor decentrale niveaus zijn niet toe te wijzen aan digitalisering specifiek; het betreft reacties op de verslechterde veiligheidssituatie in het algemeen. Bovendien is het goed mogelijk dat de algemene verandering in het bestuurlijke paradigma ook zijn weg naar de krijgsmacht heeft gevonden. Hoe dan ook, het heeft een nadruk op *samenwerking*, *integraliteit* en *vernetwerking* van de krijgsmacht tot gevolg.

Wat wél aan digitalisering specifiek kan worden toegeschreven, is de noodzaak tot samenwerking met technologiebedrijven. De ontwikkeling van digitale technologieën heeft geleid tot revolutionaire veranderingen in de manier waarop de kerntaken van de krijgsmacht verricht dienen te worden. De krijgsmacht *moet* meedoen, en komt er niet onderuit producten af te nemen van, en taken te delen met, private partijen. Dit alles is ongekend vanuit de producent-klantrelatie die de krijgsmacht met andere partijen ten aanzien van (bijvoorbeeld) materieel heeft; in veel gevallen wordt het beheer en onderhoud daarvan door de krijgsmacht zelf verricht, en gaan de ontwikkelingen veel minder snel dan bij de nieuwe technologieën.

5.2.1 Maatregelen ten aanzien van digitalisering van dreigingen

Net als bij de politionele macht zijn de maatregelen van de krijgsmacht, met betrekking tot de digitalisering van dreigingen, zonder uitzondering onderdeel van bredere pakketten aan maatregelen om de hoofdtaken van de krijgsmacht verbeterd te kunnen uitvoeren. Naast investeringen in mensen en middelen is er een sterke focus op versterkte nationale en internationale samenwerking, onder meer met civiele autoriteiten, maatschappelijke organisaties, bedrijven, strategische partners en bondgenoten. Maatregelen zijn ook hier vooral bedoeld om *weerbaarheid* te verhogen, en behelzen onder andere[100]:

- Uitbreiding van de cybercapaciteit om een grotere rol te kunnen vervullen bij de bescherming van het land tegen digitale dreigingen. Dit staat ook vermeld in de GBVS.
- Vernieuwing van de Defensie Cyber Strategie in samenhang met de Nationale Cybersecurity Agenda.
- Sensoren en informatiesystemen worden aan elkaar gekoppeld om het informatiegestuurde optreden te verbeteren. In dit kader wordt ook fors geïnvesteerd in de IT-infrastructuur en de inlichtingen-, verzamel- en analysecapaciteit (inclusief MIVD).
- Samen met het ministerie van J&V wordt de civiel-militaire samenwerking herijkt. Met andere veiligheidspartners wordt een zo dekkend mogelijk overzicht opgesteld van relevante civiele en militaire capaciteiten voor nationale crisisbeheersing en de ondersteuning bij rampenbestrijding.
- Samen met het ministerie van J&V en betrokken bedrijven wordt in kaart gebracht welke bijstand in geval van nood nodig is ter bescherming van de vitale infrastructuur en voor de digitale veiligheid.
- De Defensie Industrie Strategie wordt dit jaar geactualiseerd. Deze zal uiteen zetten hoe met het ministerie van EZK innovaties gaan worden aangejaagd in het

[100] zie https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2018/03/26/defensienota-2018/210318+Defensienota+definitief.pdf

kader van het Topsectorenbeleid. Bovendien zal deze een basis bieden voor versterking van de samenwerking van het bedrijfsleven.

- Er wordt geïnvesteerd in kennisopbouw op het gebied van cyber, informatiegestuurd optreden, slagkracht in het land-, zee- en luchtdomein en nieuwe technologieën, zoals kunstmatige intelligentie, robotica, 3D-printing en bio- en nanotechnologie.

Om recht te kunnen doen aan het veranderde dreigingsbeeld en de verslechterde veiligheidssituatie, benadrukt de minister dat maatregelen onderdeel moeten zijn van een integrale aanpak (hij spreekt van maatwerk, proportionaliteit en aandacht voor de verschillende belangen). De maatregelen dienen *"een maatschappij-brede aanpak waarbij overheidsorganisaties, veiligheidsdiensten, de krijgsmacht, bedrijfsleven en maatschappelijke organisaties actief worden betrokken bij de bescherming van de nationale veiligheidsbelangen"* te betreffen[101].

5.2.2 Fiscale, Politieke en Bestuurlijke (de-)centralisatie?

Zoals het historisch overzicht in hoofdstuk 2 reeds duidelijk maakt, is de krijgsmacht na enkele eeuwen van professionalisering in steeds grotere mate een hiërarchische, gecentraliseerde organisatie geworden. De laatste decennia van bezuinigingen hebben dit nog versterkt; de autonomie die krijgsmachtonderdelen nog hadden (bijvoorbeeld op het gebied van personele inrichting en beheer[102]) is in de bezuinigingsronden steeds verder beknot (WRR, 2017). In 2005 werd de functie van Commandant der Strijdkrachten in het leven geroepen; een overkoepelende functie, direct onder de minister en verantwoordelijk voor de aansturing van de commandanten der Zee- Land-, en Luchtstrijdkrachten opdat planning, aansturing en de organisatie van materieel centraler geregeld zou kunnen worden.

Met de nieuwe investeringen in de krijgsmacht lijkt het tij te zijn gekeerd ten aanzien van sommige indicatoren voor (de-)centralisatie; decentrale actoren krijgen meer autonomie ten aanzien van budgetten, beheer en personeel, zoals blijkt uit (onder andere) de woorden van Commandant der Strijdkrachten Bauer (§5.2) en de brief van de Minister van Defensie, aangaande de vaststelling van de begroting voor 2019[103]. Commandant van de landmacht Beulen illustreert[104] hoe hernieuwde flexibiliteit ook ten goede kan komen aan de cybercapaciteiten van de krijgsmacht:

> *"'Iemand van 140 kilo en 1,60 meter verschijnt voor mijn aannamecommissie. Die nemen we volgens het boekje niet aan. Maar wat als dat nou een van de vijf beste hackers van Nederland is? Precies. We moeten bedenken: wat moet iemand kunnen? Dan interesseert mij die 140 kilo niet meer.' Nu niet langer elk dubbeltje moet worden omgedraaid, kunnen commandanten zich ook veroorloven weer aandacht te hebben voor het effectief zijn."*

Op basis van deze bevindingen kan niet geconcludeerd worden dat de krijgsmacht ineens een sterk decentrale organisatie is. Immers, het gros aan budgettaire en financiële besluiten en algemene beleidsvoering is centraal belegd, en de krijgsmacht kent al eeuwenlang een sterke top-down command-and-controlstructuur (anders dan, bijvoorbeeld, de situatie in de vijftiende

[101] zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen/tk-tegengaan-statelijke-dreigingen.pdf

[102] zie https://www.ftm.nl/artikelen/reorganisaties-braken-slagkracht-defensie

[103] zie https://zoek.officielebekendmakingen.nl/kst-35000-X-140.pdf

[104] zie https://www.groene.nl/artikel/de-wasmachine-is-gaan-roesten

eeuw, toen huurlingenleiders vooral de belangen van hun manschappen vertegenwoordigden bij de inhuurder). 'Autonomie' als concept paste de laatste eeuwen eigenlijk niet bepaald bij de krijgsmacht, waarin discipline als een van de belangrijkste deugden wordt gezien. Osiel (1988, p.1011-2) relateert de massa-oorlogen van negentiende en twintigste eeuw ook aan de noodzaak tot discipline, en de ongewenstheid van autonomie:

> *"Modem industrial capitalism, in some postmodern views, so alienates the worker-soldier from the possibility of humane social relations that his ability to exercise meaningful moral autonomy is greatly weakened, if not eliminated. In other words, the severe hierarchy and regimentation experienced by subordinates in contemporary civilian and military workplaces belie the very conception of self, as free and rational, autonomously choosing its course of action, on which the modern law of manifest illegality has come to rest. Warfare is no longer "a game of skill [in which] all the players were skillful. It thus no longer allows much space for individual heroism, particularly that entailed in resistance to imprudent or atrocious orders, having become instead "a matter of grinding mass against mass."*

Discipline dient oorspronkelijk om de autonomie van het individu te beknotten, opdat grote aantallen van militairen beheersbaar waren. In moderne oorlogen worden gevechten echter vaker gevoerd tussen kleinere eenheden en soms zelf individuele militairen (al dan niet met de beschikking over moderne technologieën als (semi-)autonome wapensystemen), waardoor autonomie aan belang heeft gewonnen (De Vries, 2015). 'Skill', individuele professionaliteit, en street-level bureaucracy, wat volgens Osiel eerder nog aan belang verloor, is tegenwoordig weer veel belangrijker. Niet iedereen hoeft dezelfde taken te verrichten, en steeds vaker is behoefte aan specialistische kennis en skills omdat met steeds ingewikkelder en specifieker materieel wordt gewerkt en specifieke operaties worden uitgevoerd. Dit geldt momenteel in het bijzonder ten aanzien van autonome wapensystemen; een van de manieren waarop de krijgsmacht en digitalisering elkaar kruisen. De AIV heeft in 2015 een advies ten aanzien van autonome wapensystemen uitgebracht[105], waarin onder meer wordt gewezen op de gevolgen van de inzet autonome wapensystemen. Zo vraagt dit onder meer andere, meer specialistische vaardigheden op technisch, ethisch, en strategisch gebied. Het voornaamste advies van de AIV benadrukt het belang van 'betekenisvolle menselijke controle' ten aanzien van de inzet van autonome wapensystemen (AIV, 2015, p. 35):

> *"Betekenisvolle menselijke controle omvat (ten minste) de volgende drie elementen:*
> - *Mensen maken geïnformeerde, bewuste keuzes over het gebruik van wapens;*
> - *Mensen hebben adequate informatie om te verzekeren dat het geweldsgebruik conform de eisen van het internationaal recht geschiedt, gegeven de kennis die zij hebben over het doel, over het wapen en over de context waarin de inzet van het wapen plaatsvindt;*
> - *Het wapen is ontworpen en in een realistische operationele omgeving getest en mensen zijn voldoende getraind, om het wapen verantwoord te kunnen inzetten."*

Hieruit spreekt de noodzaak tot specifieke kennis en de autonomie om keuzes te maken omtrent inzet van dergelijke systemen. Hoewel er ongetwijfeld protocollen voor kunnen worden opgesteld, kunnen dergelijke besluiten niet volledig top-down worden genomen. Immers, er kunnen zich situaties voordoen waarin de expertise van de bedienaar van de technologie de expertise van commandanten (of actoren met hogere rang) in hoge mate overtreft (AIV, 2015). Hoe ingewikkelder de te gebruiken technologie wordt, hoe verder de

[105] zie https://aiv-advies.nl/88j/publicaties/adviezen/autonome-wapensystemen-de-noodzaak-van-betekenisvolle-menselijke-controle

bedienaars van die technologie dienen te professionaliseren en hoe meer ruimte er nodig gaat zijn voor deze vorm van street level bureaucracy.

Waar de krijgsmacht dus overwegend als gecentraliseerde organisatie gezien kan worden en dat niet op het punt staat drastisch te veranderen, zijn er met de nieuwe investeringen, en ten gevolge van de steeds grotere rol die technologie speelt, wel bewegingen richting decentralisatie te constateren. Ten aanzien van de digitalisering van wapensystemen valt de decentralisatie direct toe te schrijven aan die digitalisering. Ten aanzien van de meer algemene grotere zeggenschap voor decentrale actoren over beheer, personeel en materieel is een en ander meer een gevolg van het hernieuwde belang van de krijgsmacht (en die nieuwe investeringen dientengevolge). Ook hier is het goed mogelijk dat de algemene bestuurlijke NPG-trend meespeelt; grotere autonomie, vertrouwen in professionals, samenwerking en integraliteit zijn kenmerkend voor diens bestuurlijke repertoire.

5.2.3 Deelconclusie: beantwoording deelvraag 4b

Het tweede deel van de vierde deelvraag van dit onderzoek betreft de vraag wat de gevolgen van digitale dreigingen zijn voor de organisatie, taken en verantwoordelijkheden van de krijgsmacht. De bovenstaande analyse laat zien dat digitalisering als macrotrend één van de factoren betreft (naast andere trends) die hernieuwde investeringen in de krijgsmacht tot gevolg hebben. Digitalisering is daarmee dus ten dele verantwoordelijk voor het hernieuwde belang van de krijgsmacht, mede vanwege het aandeel die de ontwikkeling heeft in de verslechterde veiligheidssituatie van Nederland.

Een meer directe invloed die digitalisering op de krijgsmacht heeft, betreft de technologische revolutie in de manier waarop kerntaken van de krijgsmacht worden uitgevoerd. AI, (semi-)autonome wapensystemen, big data, robotica en bio- en nanotechnologie dwingen de krijgsmacht mee te gaan in de wapenwedloop die op dit gebied aan de gang is, en hiertoe moet de samenwerking gezocht worden met internationale private organisaties. Deze raken derhalve betrokken bij de uitvoering de taken van de krijgsmacht. Als zodanig heeft digitalisering dus, ook ten aanzien van de krijgsmacht, een vorm van pluralisering tot gevolg.

De beweging richting decentralisatie op sommige indicatoren kan worden verklaard door het totaal aan hernieuwde investering ten gevolge van hernieuwd belang; de noodzaak tot specifieke kennis en skills; en het huidige algemene bestuurlijke repertoire dat sterk waarde hecht aan samenwerking en integraliteit. De geconstateerde decentralisatie betreft echter een 'kleine stap' op het continuüm; over de breedte gezien blijft de krijgsmacht een sterk gecentraliseerde organisatie.

5.3 Veranderende dreiging en de rol van bedrijven

Digitalisering als macrotrend; de 'digitalisering van bijna alles', waarbij nagenoeg alles een computer wordt, verbonden met het internet, wordt door Schneier (2018) als gevolg gezien van markteconomische overwegingen. Hij redeneert als volgt (p.6-7):

> *"As the cost of computerized devices goes down, the marginal benefit -in either features provided or surveillance data collected- necessary to justify the computerization also goes down. The benefit could be to the user in terms of additional features, or to the manufacturer in terms of learning about and marketing to its user base. At the same time, chip suppliers are moving away from making specialty chips and towards making general-purpose, mass-produced, cheaper chips. As these embedded computers become standardized, it will be less expensive for manufacturers to include connectivity than to remove it."*

En, als gevolg daarvan:

> *"Everything is becoming one complex hyper-connected system in which, even if things don't interoperate, they're on the same network and affect each other. [...] Start with the IoT or, more generally, cyberphysical systems. Add the miniaturization of sensors, controllers, and transmitters. Then add autonomous algorithms, machine learning, and artificial intelligence. Toss in some cloud computing, with corresponding increases in capabilities for storage and processing. Don't forget to include Internet penetration, pervasive computing, and the widespread availability of high-speed wireless connectivity. And finally, mix in some robotics. What you get is a single global internet that affects the world in a direct physical manner. It's an internet that senses, thinks and acts."*

Naast dat alle IoT-devices, sensoren, controllers, transmitters, AI, software en andere fysieke en nonfysieke noodzakelijkheden voor het bestaan van deze netwerken geproduceerd en geüpdate worden door (grote) technologiebedrijven, is de beschreven onderlinge connectiviteit essentieel voor nagenoeg alle vitale en non-vitale sectoren en domeinen van de moderne samenleving, die volledig afhankelijk is geworden van deze digitale middelen, waarbij security-by-design vaak geen eerste prioriteit is geweest[106]. Binnen deze sectoren zijn dikwijls geen analoge alternatieven meer beschikbaar als terugvalopties. Dit maakt de afhankelijkheid van gedigitaliseerde processen en systemen zo groot, dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade[107].

Eerder is reeds geconstateerd dat deze enorme vernetwerking het onderscheid tussen interne en externe veiligheid naar het verleden verwijst. Echter, ook binnen dit onderscheid doen zich incidenten en dreigingen voor, waarbij de rol van private organisaties steeds vaker onderwerp van gesprek is, vanwege hun aandeel in de verspreiding of materialisatie van de dreigingen. Enkele voorbeelden:

- De rol van Microsoft ten aanzien van het updaten van essentiële systemen, ook wanneer dit niet automatisch gebeurt of wordt uitgesteld, was onderwerp van discussie rondom de schade die de WannaCry-aanval aanrichtte bij ziekenhuizen in het Verenigd Koninkrijk[108];
- Chips van fabrikant Intel blijken fouten te bevatten waardoor miljoenen computers kwetsbaar zijn voor datalekken[109];
- Videoplatform Youtube gaat strenger controleren op de inhoud van materiaal dat wordt geüpload, om te voorkomen dat content die schadelijk is voor publieke waarden zich verspreidt[110];
- Vresesorganisatie PAX waarschuwt dat de initiatieven die Microsoft en Amazon op het gebied van defensietechnologie voor het Pentagon ontplooien zeer zorgwekkend zijn[111]. Microsoft gaf in een eerder stadium juist aan (nadat Google zich had teruggetrokken) door te willen gaan met de samenwerking, omdat 'de mensen die het land verdedigen de steun verdienen en nodig hebben' en om 'publiek debat over verantwoordelijk gebruik van technologie' aan te jagen[112];

---

[106] zie https://www.dcypher.nl/sites/default/files/uploads/documents/Rapport%20_Digitale%20Hygiene%20Nederland%20-%20Juni%202018_.pdf

[107] zie https://www.nctv.nl/binaries/Nationale%20Veiligheid%20Strategie%202019_tcm31-393099.pdf

[108] zie bijvoorbeeld https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs

[109] zie bijvoorbeeld https://www.rtlz.nl/tech/artikel/4805366/intel-chips-processor-hack-kwetsbaar-lek-bitdefender

[110] zie bijvoorbeeld https://www.nrc.nl/nieuws/2019/06/05/youtube-gaat-strenger-optreden-tegen-haatfilmpjes-a3962758

[111] zie bijvoorbeeld https://www.paxforpeace.nl/media/files/pax-report-killer-robots-dont-be-evil.pdf

[112] zie https://blogs.microsoft.com/on-the-issues/2018/10/26/technology-and-the-us-military/

- Gebrekkige privacybeveiliging bij Facebook leidde ertoe dat de data van wereldwijd tot wel 87 miljoen mensen (89 duizend mensen in Nederland) in handen kwam van onderzoeksbureau Cambridge Analytica, dat een omstreden rol speelde rondom de Amerikaanse verkiezingen van 2016[113]. Het leidde ertoe dat Facebook-topman Zuckerberg zich moest komen verantwoorden bij het Amerikaanse Congres en het Europees Parlement;
- Omstreden internetforum 8chan wordt, nadat aanslagplegers zich lieten inspireren door posts op het forum en zelf schadelijke brieven en manifesten plaatsen, niet meer door netwerkprovider Cloudfare ondersteund[114].

Bedrijven hebben vanwege hun producten en diensten dus een grote rol in openbare orde en nationale veiligheid. Dit maakt ze tot een onvermijdelijke netwerkpartner voor de traditionele veiligheidsapparaten. Wanneer de bedrijven taken ten aanzien van de openbare orde en nationale veiligheid op zich nemen, nemen ze dus eigenlijk taken op zich die snijvlakken hebben met de taken van politie en krijgsmacht. Bovendien zijn de bedrijven niet enkel netwerkpartner, ze zijn ook toeleveranciers voor essentiële nieuwe technologieën waarmee krijgs- en politionele macht hun kerntaken uitvoeren: zaken als AI, Big Data, en robotica worden gebruikt om criminaliteit te voorspellen[115], autonome wapensystemen te laten functioneren en surveillancepraktijken (Smits en Besters, 2011). Ten slotte hebben de bedrijven vanwege hun kernactiviteiten zicht op activiteiten en handelingen die (omdat ze via dergelijk grote publieke platforms worden verricht) door andere staten worden verricht[116]. Dientengevolge dienen ze voor veiligheidsdiensten en het publiek als surveillanten.

5.3.1 Voorschriften versus gedrag

De belangrijke rol die private organisaties spelen ten aanzien van de digitalisering van veiligheidszorg roept vragen op rond legitimiteit (Phelps, 2014) en de mate waarin overheden op toch nog verantwoordelijk kunnen worden gehouden voor de handelingen van dergelijke bedrijven (Jinks, 2003). Immers, hoe het precies zit met zaken als verantwoordelijkheden, aansprakelijkheidsstelling, eigenaarschap, de invloed op publieke waarden is vaak onduidelijk. Zoals hierboven geïllustreerd nemen zien bedrijven hier en daar hun verantwoordelijkheden toenemen en handelen ze daar ook naar, maar deze bottom-upbenadering kenmerkt zich door vrijblijvendheid en eigen interpretatie. Vanuit de overheid bestaat er ten aanzien van dergelijke vraagstukken nog geen centrale regie en is er nog geen coherent technologiebeleid, zoals dat in staten als Frankrijk, Rusland en China wel in grotere mate het geval is[117]. Dit betekent dat er geen hiërarchische structuur bestaat van waaruit (re-)organisatie en verantwoordelijkheidsstelling van deze onderdelen van de veiligheidssituatie in Nederland kan plaatsvinden[118]. Dit is ook geen gemakkelijke aangelegenheid. Immers, veiligheid wordt veelal gezien als de keerzijde van de medaille; de 'andere kant' van innovatie. Onder deze noemer gaan

[113] zie bijvoorbeeld https://www.trouw.nl/nieuws/gegevens-89-000-nederlandse-facebookgebruikers-in-handen-cambridge-analytica~bc1c2703/

[114] zie bijvoorbeeld https://tweakers.net/nieuws/155762/cloudflare-stopt-ondersteunen-van-omstreden-forum-8chan.html

[115] zie bijvoorbeeld https://www.politie.nl/nieuws/2017/december/9/01-big-data-een-grote-impuls-bij-opsporing.html

[116] zie bijvoorbeeld https://nos.nl/artikel/2298211-china-met-spam-en-nepaccounts-actief-in-hongkong-zeggen-twitter-en-facebook.html

[117] zie bijvoorbeeld https://www.nrc.nl/nieuws/2019/06/11/nederland-moet-haast-maken-met-coherent-technologiebeleid-a3963190

[118] zie https://www.tweedekamer.nl/downloads/document?id=3b6b4589-3021-4604-a28b-5338757c1959&title=Motie%20van%20het%20lid%20Verhoeven%20c.s.%20over%20het%20instellen%20van%20een%20onderzoekscommissie.pdf

de technologische ontwikkelingen door bedrijven in een dermate hoog tempo dat ze recht doen aan het predikaat 'vierde industriële revolutie' (Schwab, 2017). Op de thema's 'cognitie' en 'autonomie' zorgt dit echter voor waarschuwingen voor onbeheersbaarheid en ongewenst gedrag[119]. Dit maakt dat overheidsbeleid constant dient te manoeuvreren tussen 'kansen' en 'risico's'[120].

Het invoeren van wet- en regelgeving ten behoeve van compliance door bedrijven wordt ten tweede ernstig bemoeilijkt door het feit dat (grote) techbedrijven zich vaak in andere staten en dus andere jurisdicties bevinden. Bovendien zijn sommige technologiebedrijven zo groot dat overheden maar moeilijk grip op ze kunnen krijgen[121], en is van veel kleinere technologiebedrijven (zoals producenten van hard- en software) bij overheden onvoldoende duidelijk in hoeverre hun producten en diensten van invloed zijn op de nationale veiligheid. De focus ligt immers op sectoren en bedrijven die een rol spelen ten aanzien van vitale infrastructuur en belangen. Overige bedrijven worden gestimuleerd zoveel mogelijk hun eigen veiligheid en verantwoordelijkheid vorm te geven (NCTV, 2018a). Maar: veel van deze bedrijven hebben ook te maken met kwetsbaarheden in hun soft- en hard die tot grote schade kunnen leiden. Zij zijn nu vaak op zichzelf aangewezen, terwijl het digitale fundament waarop deze bedrijven hun activiteiten bouwen vaak hetzelfde is als dat van de vitale infrastructuur[122];

Pogingen om technologiebedrijven verantwoordelijkheid te laten nemen voor hun aandeel in de veiligheidszorg worden inmiddels wel ondernomen. Zo wil de Britse regering directieleden van sociale-mediabedrijven persoonlijk verantwoordelijk kunnen houden wanneer er schadelijke content via hun websites wordt verspreid. In Nederland is er de 'Roadmap Digitaal Veilige Hard- en Software'[123] waarmee gepoogd wordt onveiligheden en kwetsbaarheden in hard- en software te detecteren en aan te pakken, De Franse regering stelt ten aanzien van grote technologiebedrijven een zogenaamde 'digitaks' in[124], en ook andere Europese landen en de EU ondernemen verschillende initiatieven om de technologiebedrijven tot compliance te bewegen[125].

In conclusie: technologiebedrijven hebben een grote impact op, en maken een belangrijk deel uit van de veiligheidszorg ten aanzien van digitalisering. 'Van bovenaf' en 'van onderaan' worden ook pogingen ondernomen om verantwoordelijkheid voor veiligheidsbelangen te nemen, maar echte sturing ontbreekt.

5.3.2 Deelconclusie: beantwoording deelvraag 4c

Het derde deel van de vierde deelvraag in deze thesis is 'wat zijn de gevolgen van digitale dreigingen voor de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor private partijen (bedrijven)?'. De bovenstaande (sub-)paragrafen maken inzichtelijk dat ten gevolge van digitalisering ook de belangrijkste veroorzakers daarvan een belangrijk aandeel hebben verworven in de veiligheidszorg ten aanzien van digitalisering: technologiebedrijven.

---

[119] zie https://www.thehaguesecuritydelta.com/media/com_hsd/report/216/document/ANV-Horizonscan-Nationale-Veiligheid-2018.pdf

[120] zie https://www.wrr.nl/binaries/wrr/documenten/brieven/2018/06/11/adviesaanvraag-artificial-intelligence/Adviesaanvraag-kunstmatige-intelligentie.pdf

[121] zie https://www.nrc.nl/nieuws/2018/01/23/hoog-tijd-dat-overheden-techmonopolies-gaan-aanpakken-a1589467

[122] zie https://www.nctv.nl/onderwerpen_a_z/csbn/belangen.aspx

[123] zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software/Roadmap+Digitaal+Veilige+Hard-+en+Software.pdf

[124] zie bijvoorbeeld https://www.volkskrant.nl/nieuws-achtergrond/frankrijk-voert-digitaks-in-voor-techreuzen-en-zet-daarmee-de-relatie-met-de-vs-onder-spanning~b89b53d7/

[125] zie bijvoorbeeld https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html

Overige bedrijven, al dan niet onderdeel van de vitale infrastructuur, maken ook gebruik van de producten en diensten die samen zorgen voor de 'vernetwerking van alles'. Hun verantwoordelijkheden lijken meer op die van burgers, zoals hieronder besproken zal worden.

Technologiebedrijven laten regelmatig zien zich bewust te zijn van hun verantwoordelijkheden ten aanzien van de veiligheidszorg, maar hun gedrag ten aanzien van het nemen van die verantwoordelijkheden kenmerkt zich door vrijblijvendheid en eigen interpretatie. Hoewel overheidsorganisaties pogen meer centrale coördinatie en sturing aan te brengen, vindt praktisch gezien dus een versnippering en vertroebeling van verantwoordelijkheden, besluitvorming, kennis en autoriteit plaats. In combinatie met de netwerkpositie die de bedrijven ten aanzien van de traditionele veiligheidsapparaten bekleden, betekent de digitalisering van dreigingen een pluralisering en decentralisering van de veiligheidszorg, vanwege de rollen en verantwoordelijkheden voor private organisaties.

5.4 Veranderende dreiging en de rol van burgers

De vierde case in dit onderzoek betreft de rollen en verantwoordelijkheden van burgers ten aanzien van de digitalisering van dreigingen. Eerder werd al geconstateerd dat burgers al lange tijd vooral aan de 'ontvangende kant' van de veiligheidszorg staan, en dat enige bemoeienis in de veiligheidszorg eerder als overtreding dan als legitieme bijdrage wordt aangemerkt. Digitalisering heeft er echter voor gezorgd dat een immens deel van de genetwerkte apparaten en systemen in handen van burgers[126] zijn; hun computers en telefoons, 'slimme apparaten', medische applicaties en zo verder. Dit leidt ertoe dat burgers een hernieuwde verantwoordelijkheid krijgen toebedeeld ten aanzien van collectieve veiligheidsoverwegingen.

Doen burgers ten aanzien van 'fysieke' veiligheidszorg niets zelf? Zeker wel: wet- en regelgeving; verzekeraars; waardering van lijf, leden en privé-eigendommen; en onveiligheidsgevoelens van mensen zelf hebben ertoe geleid dat burgers hun huizen op slot doen, autogordels dragen, hun kinderen inenten, spullen niet onbeheerd achterlaten en geen scherpe voorwerpen mee proberen te nemen in vliegtuigen. Mensen zijn dus wel gewend in enige mate voor hun eigen veiligheid te zorgen. Echter, al deze maatregelen leiden vooral tot grotere veiligheid voor mensen zelf (en wellicht hun directe omgeving). Niemand sluit zijn huis af vanwege de vernetwerking van huizen, en de gevolgen die inbraak kan hebben voor die complete netwerken. De meeste huizen zijn immers ook niet middels doorgangen met elkaar verbonden. Gedragswetenschappers hebben inmiddels inzichtelijk gemaakt dat mensen in redelijke mate bereid zijn veiligheidsmaatregelen te nemen om zichzelf en hun naasten te beschermen, maar nauwelijk voor het algemeen belang (Donahue et al., 2014).

De digitalisering van de maatschappij heeft kwetsbaarheden met zich meegebracht die conceptueel raken aan de hierboven beschreven fysieke veiligheidskwesties. Immers, IoT-apparaten, mobiele telefoon en computers zijn eigendommen die veelal onder verzekeringen vallen. Dergelijke apparaten bieden mensen echter -veelal als secundaire functionaliteit!- de mogelijkheid zich te begeven in het digitale domein waar zich (zoals inmiddels bekend) ook allerhande dreigingen voordoen. Om hier schade te voorkomen, dienen mensen ook zo hun maatregelen te nemen: het gebruiken van goede wachtwoorden; regelmatig updaten; niet op vreemde links klikken; en regelmatig backups maken. Voor (de consequenties van) hun digitale gedrag worden mensen in steeds grotere mate zelf verantwoordelijk gehouden[127]: van mensen

[126] in deze paragraaf kan naast 'burgers' ook bedrijven gelezen worden, waarbij het gaat om bedrijven die geen onderdeel uitmaken van de techsector. Denk aan de bakker op de hoek, een supermarkt of een sportschool.

[127] zie bijvoorbeeld http://www.nederlandveiligonline.nl/

wordt 'cyberhygiëne' verwacht. De Nationale Cyber Security Strategie II (NCTV, 2013, p. 20) ziet deze cyberhygiëne als het toepassen van basis-veiligheidsvereisten, en stelt:

> *"Van burgers mag een zekere basis-cyberhygiëne en bekwaamheid worden verwacht als zij ICT gebruiken, bijvoorbeeld bij het surfen op het web. Denk aan voorzichtig zijn met persoonlijke gegevens, het uitvoeren van updates, het gebruik van sterke wachtwoorden en het in evenwicht brengen van functionaliteit en cybersecurity".*

Het beroep dat op burgers wordt gedaan is niet onomstreden[128]. Immers, DDoS-aanvallen op vitale sectoren worden ongemerkt uitgevoerd middels in botnets ingelijfde, onvoldoende beveiligde IoT- apparaten, die veelal in handen van particulieren zijn (Van Eeten et al., 2011). Met de verwachting dat burgers in staat zijn hun eigen apparaten, systemen en netwerken veilig te houden, worden zij mede verantwoordelijk gemaakt voor een belangrijk deel van de digitale infrastructuur waarlangs dreigingen voor de nationale veiligheidsbelangen zich kunnen verspreiden en materialiseren.

Waar mogelijk wordt in de fysieke wereld (conform het heersende bestuurlijke paradigma) ingezet op co-productie en co-creatie van publieke diensten door burgers, bedrijven en overheidsinstellingen in samenwerkingsverband. Zo ook bij de fysieke politietaken. Denk aan getuigenoproepen, het verstrekken van beeldmateriaal, hulp bij zoekacties en opsporingsactiviteiten (Meijer et al., 2013). In het digitale domein zouden bepaalde vormen van burgerparticipatie gebruikt kunnen worden om expertise en kennis van burgers te gebruiken om tekortkomingen hierin bij de politionele macht op te vangen (Knapen, 2017). Chang et al. (2018) wijzen op co-productie-initiatieven van burgers om de beperkte capaciteiten van staten om in cyberspace te patrouilleren, aan te vullen. De hoeveelheid illegale activiteiten in cyberspace zorgt voor meer dreiging dan overheden aankunnen. Individuen en organisaties zijn zich bewust van dit tekort aan capaciteit bij de overheid en proberen soms zelf in dit tekort te voorzien. Niet al deze niet-statelijke antwoorden op cybercrime passen echter binnen de grenzen van de wet. Burgers, commerciële bedrijven en non-profit organisaties kunnen allemaal in posities komen dat ze online illegaliteiten tegenkomen en herkennen, en ze aangeven bij de autoriteiten. Van tijd tot tijd nemen individuen het heft echter in eigen handen. In plaats van simpelweg wetshandhavers te wijzen op illegale activiteit, kiezen 'vigilante burgers' ervoor in hun eentje de overtreder aan te pakken[129]. Zij plegen eigenrecht en denken dat ze in een positie zijn om criminelen te straffen, ook middels criminele middelen.

Betrokkenheid van burgers bij digitale veiligheid kan in bepaalde mate nuttig en wenselijk zijn. Het is echter belangrijk om met criteria te komen voor het inschatten van de gepastheid van co-productie in cybersecurity, net als in de fysieke wereld. De Nederlandse politie leidt inmiddels burgers op tot 'dark-web-surveillanten', en vraagt hen derhalve dus onderdeel uit te maken van de bestrijding van digitale en gedigitaliseerd dreigingen[130]. Ook de krijgsmacht tracht digitaal vaardige burgers te betrekken, en stelt sinds lange tijd de deuren weer open om burgerpersoneel te werven, voornamelijk op technologisch vlak[131]. Digitalisering heeft zogezegd tot gevolg gehad dat burgers, zij het met enige haken en ogen, inmiddels een integraal onderdeel zijn geworden van de veiligheidszorg. De manier waarop dat gebeurt (trainingen, vrijwillige inzet van specialisten, aanwijzing van 'surveillanten') doet denken aan de

[128] zie ook https://www.nrc.nl/nieuws/2017/05/15/laat-cyberveiligheid-niet-aan-burger-over-9097654-a1558752

[129] zie bijvoorbeeld https://www.ad.nl/nieuws/anonymous-zet-rick-astley-in-als-wapen-tegen-is~af9efe4e/

[130] zie https://tweakers.net/plan/2022/politie-wil-hulp-van-burger-bij-bestrijden-cybercrime.html

[131] zie bijvoorbeeld https://www.youtube.com/watch?v=lUKR0Eg31Kw

manier waarop in de achttiende eeuw nachtwachten en marktopzichters in het fysieke domein een oogje in het zeil hielden, en de autoriteiten konden waarschuwen in geval van onraad.

5.4.1 Voorschriften versus gedrag

Burgers worden aangesproken op hun eigen verantwoordelijkheid ten aanzien van digitale veiligheid. Middels overheidscampagnes en websites van samenwerkingsverbanden worden mensen ertoe aangespoord toch vooral maatregelen te nemen om zichzelf en hun bezittingen te beschermen[132]. Desgevraagd laten burgers zelf weten zichzelf óók als hoofdverantwoordelijke te zien voor de eigen digitale veiligheid[133]. Het bewustzijn ten aanzien van de waarschijnlijkheid van cyberdreigingen en de nadruk die men op de eigen verantwoordelijkheid legt, leidt er echter niet zonder meer toe dat men er ook in slaagt de veiligheid van eigen apparaten, gegevens, netwerken en systemen te garanderen. Uit het verleden is gebleken dat een groot aantal hacks en andere onveilige situaties heeft plaatsgevonden op basis van relatief eenvoudige kwetsbaarheden zoals het hebben van een standaardwachtwoord[134], onveilige verbindingen en/of onjuiste technische inrichting (van software). Ondanks de (inter-)nationale aandacht, campagnes en persberichten is zelfs een toename van deze kwetsbaarheden te constateren: van Nederlanders tussen de 18 en 80 jaar weet 21% niet wat *phishing mails* zijn, 43% weet niet wat *malware* is, en 59% weet niet wat een DDoS-aanval is[135], voorlichtingscampagnes ten spijt. Dit, terwijl de verspreiding van deze digitale dreigingen staat of valt bij de apparaten, netwerken en gedragingen van burgers. Hierbij valt op dat Nederland eenzelfde trend laat zien als de rest van de wereld[136], terwijl het een van de meest gedigitaliseerde landen ter wereld is en men zichzelf en behoorlijke mate van verantwoordelijkheid toedicht.

Burgers beschikken klaarblijkelijk niet over de bereidheid enerzijds, of de vaardigheden anderzijds, om te voldoen aan het beroep tot cyberhygiëne dat op hen wordt gedaan. Dit leidt er vaak toe dat zij door overheid en bedrijfsleven worden geclassificeerd als 'lui' of 'onverantwoordelijk'. Echter, deze non-compliance kan eigenlijk nauwelijks als verrassing gelden. Immers, vanuit rationeel oogpunt is het niet constant opvolgen van cybersecurity-instructies heel logisch: het leidt tot indirecte kosten (tijd en moeite) die vaak niet opwegen tegen het genomen risico, en lijsten met adviezen en instructies[137] gaan uit van *worst case scenario's* en zijn vaak complex en tegenstrijdig (Herley, 2009). Wanneer mensen overigens wél aan alle veiligheidsadviezen gehoor geven, dreigt zelfoverschatting vergelijkbaar aan Adams veiligheidsparadox: men waant zich beschermd door het vertrouwen in hun beveiligingssoftware waardoor eerder risico's genomen worden. Dientengevolge gedraagt men zich minder alert én minder veilig, wat alsnog leidt tot geïnfecteerde of ingelijfde apparaten, verlies van data en verhoogde systeem- en netwerkonveiligheid (Acquisti et al., 2017).

De vraag is of de verwachting die aan burgers wordt gesteld wel zo realistisch is. Eerder is reeds besproken dat criminele, ongewenste en onveilige digitale dreigingen niet enkel vanuit medeburgers komen (waar dat bij bijvoorbeeld traditionele fietsendiefstal en intimidatie doorgaans wel nog het geval is), maar nu ook door private bedrijven of zelfs andere staten (of aan andere staten gelieerde actoren) verricht worden. Deze actoren hebben haast onmetelijk

[132] zie bijvoorbeeld https://www.alertonline.nl/tips

[133] zie https://www.alertonline.nl/media/Cybersecurity-Bewustzijnsonderzoek-Alert-Online-2018-2.pdf

[134] zie bijvoorbeeld https://fd.nl/ondernemen/1310561/gekraakte-wachtwoorden-feyenoord-verslaat-ajax-met-grote-cijfers

[135] zie https://www.alertonline.nl/media/Cybersecurity-Bewustzijnsonderzoek-Alert-Online-2018-2.pdf

[136] zie https://www.dcypher.nl/sites/default/files/uploads/documents/Rapport%20_Digitale%20Hygiene%20Nederland%20-%20Juni%202018_.pdf

[137] zie bijvoorbeeld https://www.alertonline.nl/tips

veel grotere capaciteiten dan individuele burgers om dreigingen te mitigeren. Nou zal het niet snel voorkomen dat de gemiddelde burger door een buitenlandse overheid gehackt wordt. Er zijn echter legio voorbeelden waarbij sprake is van beïnvloeding[138], intimidatie[139] of inlijving van private apparaten in botnets[140]. Nederland staat zevende op de wereldranglijst wat betreft onveilige blootstellingen via het internet. Het merendeel van de technische kwetsbaarheden zit in het gebruik van onveilige protocollen, onveilige inrichting van IT en standaardwachtwoorden (Toms, 2018).

Eerder is ten aanzien van andere vraagstukken ook reeds gebleken dat 'weten' niet automatisch leidt tot 'doen'(WRR, 2017b); specifieke vaardigheden zijn trainbaar, maar dat vraagt om flinke en langdurige investeringen[141]. Allerlei factoren kunnen eraan bijdragen dat zelfs mensen die graag willen en in de kern ook de juiste vaardigheden hebben, er toch niet in slagen te doen wat er van ze wordt gevraagd. De overheid maakt, in een ultieme poging toch het gewenste gedrag te bewerkstelligen, steeds vaker gebruik van gedragswetenschappelijke inzichten[142]. Door andere keuzes te maken ten aanzien van de 'keuzearchitectuur', kunnen mensen die om wat voor reden dan ook moeite hebben de wenselijke keuzes te maken, toch een 'duwtje in de goede richting' krijgen (zie ook §2.1.4). In het fysieke domein uit zich dat bijvoorbeeld via stickers op gezondere alternatieven in de supermarkt; belijning en bewegwijzering in het verkeer; en het vooraf zo ver mogelijk invullen van de belastingaangifte. Het digitale domein staat bol van dergelijke 'nudges', maar zeker niet altijd naar het meest veilige gedrag. Reclames, trackers en phishing-tools kunnen door kwaadwillenden gebruikt worden om mensen juist onveilig of privacygevoelig gedrag te laten vertonen (Acquisti et al., 2017). Overheden zouden, om het burgers gemakkelijker te maken zichzelf en anderen te beschermen, druk kunnen uitoefenen op technologiebedrijven om hun producten te voorzien van veiligheidsnudges, en hiertoe ook losse applicaties uit te brengen. Acquisti et al. (2017) wijzen erop dat ook ten aanzien van dergelijke technologieën labels en keurmerken tot beter geïnformeerde keuzes kunnen leiden; 'wachtwoordmeters' tot verstandiger overwegingen; en andere standaardinstellingen vanuit de fabriek voor betere standaard veiligheidsinstellingen. Op deze manieren kunnen de gedragingen van burgers mogelijk beter aansluiting vinden met de verwachting tot cyber hygiëne die aan hen gesteld wordt. Noodzakelijk, want burgers zijn met hun netwerken, apparaten en systemen een belangrijk onderdeel in de omgang met dreigingen ten aanzien van digitalisering.

5.4.2 Deelconclusie: beantwoording deelvraag 4d

Het vierde en laatste deel van de vierde deelvraag die in deze thesis beantwoord dient te worden is 'wat zijn de gevolgen van digitale dreigingen voor de taken en verantwoordelijkheden ten aanzien van veiligheidszorg voor burgers?'. De hierboven besproken bevindingen ten aanzien van gedigitaliseerde dreigingen waarmee burgers te maken krijgen, de manier waarop men daar in het algemeen mee omgaat en de verwachting die aan hen wordt gesteld, laten zien dat digitalisering ervoor zorgt dat er sinds lange tijd voor burgers weer een taak is weggelegd in de bescherming tegen dreigingen voor de nationale veiligheidsbelangen. Dreigingen kunnen ten

[138] zie bijvoorbeeld https://www.volkskrant.nl/nieuws-achtergrond/rutte-nederland-alert-op-buitenlandse-beinvloeding-verkiezingen-door-hacks~b40c41ec/

[139] zie bijvoorbeeld https://nos.nl/artikel/2296862-partners-militairen-thuis-lastiggevallen-over-missie-baltische-staten.html

[140] zie bijvoorbeeld https://www.ad.nl/tech/16-miljoen-duitsers-slachtoffer-botnet-wat-is-het-en-hoe-wapen-je-je-ertegen~a5fc5dc9/

[141] zie https://zembla.bnnvara.nl/nieuws/overheid-overschat-zelfredzaamheid-burgers

[142] zie https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2018Z00849&did=2018D01790

gevolge van digitalisering immers via apparaten, netwerken en gedragingen van burgers bijdragen aan verhoogde onveiligheid ten aanzien van vitale onderdelen van de samenleving. Burgers dienen derhalve niet enkel zichzelf en hun eigen bezittingen te beschermen, maar ook vanuit overwegingen ten aanzien van de samenleving te handelen. Aan die situatie zijn burgers niet meer gewend. De overheid kan hierop inspelen door niet enkel te appelleren aan verantwoordelijkheidsgevoel en lijstjes met instructies, maar ook door veilig handelen makkelijker en voordehandliggender te maken. Hoewel het lijkt alsof er van burgers dus weinig verwacht kan worden, wijst de praktijk uit dat burgers een belangrijk deel van de veiligheidszorg ten aanzien van digitalisering op zich dienen te nemen. Het door digitalisering toegenomen belang van deelname door burgers in de veiligheidszorg wijst op verdere pluralisering, en een sterke mate van decentralisatie.

HOOFDSTUK ZES
HOE NU VERDER?

In deze thesis is onderzoek gedaan om de volgende hoofdvraag te beantwoorden:

In hoeverre leidt de noodzaak tot controle van digitale dreigingen tot een meer gecentraliseerde, of juist meer gedecentraliseerde veiligheidszorg?

Middels een viertal deelvragen zijn hypothesen opgesteld en getoetst. In hoofdstuk 2 werden de volgende tegengestelde verwachtingen uitgesproken:

1. Hoe groter de mate waarin dreigingen digitaliseren, hoe meer *gecentraliseerd* de veiligheidszorg zal raken.
2. Hoe groter de mate waarin dreigingen digitaliseren, hoe meer *gedecentraliseerd* de veiligheidszorg zal raken.

Middels toetsend, evaluatief multiple case-study onderzoek is aan de hand van verschillende bronnen antwoord gegeven op de empirische deelvragen. Dat gebeurde ten aanzien van de onafhankelijke variabele in hoofdstuk 4, en ten aanzien van de afhankelijke variabele in hoofdstuk 5.

In dit hoofdstuk wordt ten eerste de hoofdvraag beantwoord middels reflectie op de hypothesen. Welke implicaties de uitkomsten van dit onderzoek hebben voor het bestuurskundige vakgebied en de bestuurlijke praktijk komt vervolgens aan bod, evenals een kritische reflectie op de verrichte analyse. Dit hoofdstuk sluit af met het doen van aanbevelingen voor vervolgonderzoek.

6.1 Conclusie

Digitalisering is een revolutionaire maatschappelijke en technologische ontwikkeling, waarbij niet alleen factoren omtrent communicatie en informatie zich naar het digitale domein verplaatsen, maar dat ook gebeurt met dreigingen voor de nationale veiligheidsbelangen. Digitalisering is bovendien enerzijds een van de oorzaken van een dynamisch, veranderend dreigingsbeeld. Het zorgt, samen met andere macrotrends, voor vervlechting van interne en externe veiligheid en voor steeds verdergaande samenhang tussen verschillende dreigingscategorieën ten gevolge van vernetwerking. Anderzijds betreft het een dreigingscategorie op zich, waarbinnen een veelheid aan actoren via een veelheid aan kanalen een veelheid aan doelwitten kan treffen.

Voor de politionele macht heeft dit tot gevolg dat naast de Nationale Politie een verscheidenheid aan andere actoren betrokken is geraakt bij het verrichten van politiewerk. Politiewerk ten aanzien van de digitalisering van dreigingen heeft daarmee een *gepluraliseerd* karakter gekregen, en het totale netwerk aan actoren dat de verantwoordelijkheid voor dit politiewerk op zich neemt, is sterk *decentraal* van aard. Overheidsinstellingen fungeren binnen dit netwerk als partner en facilitator, passend bij de algehele huidige bestuurlijke trend. De politionele macht zelf is met de Politiewet 2012 sterk *gecentraliseerd*. Dit kan echter maar voor een beperkt deel worden toegeschreven aan de macrotrend digitalisering. Andere ontwikkelingen hebben immers ook bijgedragen aan de reorganisatie. Ook het feit dat de politionele macht in Nederland zich in toenemende mate als *netwerkpartner* in publiek-private

samenwerkingsverbanden opstelt, kan niet exclusief aan digitalisering van dreigingen worden toegeschreven. Om digitale dreigingen te mitigeren wordt weliswaar opvallend vaak de samenwerking in netwerkverbanden gezocht, maar dit is passend bij de *bestuurlijke paradigmaverschuiving* die in veel meer domeinen dan enkel de veiligheidszorg zichtbaar is.

Digitalisering als macrotrend betreft één van de factoren (naast andere ontwikkelingen) die hernieuwde investeringen in de krijgsmacht tot gevolg hebben. Digitalisering is daarmee ten dele verantwoordelijk voor het hernieuwde belang van de krijgsmacht, mede vanwege het aandeel die de ontwikkeling heeft in de verslechterde veiligheidssituatie van Nederland. Een meer directe invloed die digitalisering op de krijgsmacht heeft, betreft de technologische revolutie in de manier waarop kerntaken van de krijgsmacht worden uitgevoerd. AI, (semi-) autonome wapensystemen, big data, robotica en bio- en nanotechnologie dwingen de krijgsmacht mee te gaan in de wapenwedloop die op dit gebied aan de gang is, en hiertoe moet de samenwerking gezocht worden met internationale private organisaties. De noodzakelijke samenwerkingsverbanden die moeten worden aangegaan impliceren ten aanzien van de taken van de krijgsmacht ook een vorm van *pluralisering*. Hierbij vinden delen van de 'krijgstaakuitoefening' dus meer decentraal plaats. De krijgsmacht zelf vertoont ook indicaties van decentralisering, maar blijft in de kern nog een zeer gecentraliseerde organisatie. De voorbeelden van decentralisering die aan de hand zijn, zijn bovendien niet zomaar toe te schrijven aan digitalisering, en passen binnen de *bestuurlijke paradigmaverschuiving*.

Technologiebedrijven hebben ten gevolge van digitalisering een belangrijk aandeel verworven in de veiligheidszorg ten aanzien van digitalisering. Hoewel zij regelmatig laten zien zich bewust te zijn van hun verantwoordelijkheden ten aanzien van de veiligheidszorg, kenmerkt hun gedrag ten aanzien van het nemen van die verantwoordelijkheden zich door vrijblijvendheid en eigen interpretatie. Hoewel overheidsorganisaties pogen meer centrale coördinatie en sturing aan te brengen, vindt praktisch gezien dus een *versnippering* en *vertroebeling* van verantwoordelijkheden, besluitvorming, kennis en autoriteit plaats. In combinatie met de netwerkpositie die de bedrijven ten aanzien van de traditionele veiligheidsapparaten bekleden, betekent de digitalisering van dreigingen een *pluralisering* en *decentralisering* van de veiligheidszorg, vanwege de rollen en verantwoordelijkheden voor private organisaties en hun losse onderlinge verbanden.

Digitalisering zorgt ervoor dat er sinds lange tijd voor burgers weer een taak is weggelegd in de bescherming tegen dreigingen voor de nationale veiligheidsbelangen. Burgers dienen derhalve niet enkel zichzelf en hun eigen bezittingen te beschermen, maar ook vanuit overwegingen ten aanzien van de samenleving te handelen. Aan die situatie zijn ze niet meer gewend, en men slaagt er momenteel ook niet in de verwachtingen tot 'cyberhygiëne' waar te maken. Hoewel dat een vrijbrief lijkt om te stellen dat er van burgers dus weinig verwacht kan worden, wijst de praktijk uit dat zij nou eenmaal een belangrijk deel van de veiligheidszorg ten aanzien van digitalisering op zich dienen te nemen, omdat de traditionele veiligheidsapparaten daar niet in slagen. Het door digitalisering toegenomen belang van deelname door burgers in de veiligheidszorg wijst op verdere *pluralisering*, en een sterke mate van *decentralisatie*.

Voor het tweetal hypothesen dat in deze thesis getoetst is, betekenen de antwoorden op de deelvragen dat de eerste hypothese dient te worden verworpen, terwijl de tweede hypothese dient te worden geaccepteerd. De enige echte vorm van centralisatie die geconstateerd is, is de invoering van de Nationale Politie middels de Politiewet van 2012. Deze is echter niet of nauwelijks te wijten aan digitalisering. Een variëteit aan andere factoren hebben een grotere rol gespeeld in de organisationele centralisatie. Puur kijkend naar digitalisering, dan kan geconcludeerd worden dat deze juist geleid heeft tot pluralisering, versnippering en, daarmee,

decentralisatie van politiewerk, vanwege de veelheid aan andere actoren die dergelijk werk op zich hebben genomen. Ook bij de krijgsmacht is er, hoewel dit een sterk gecentraliseerde organisatie betreft, eerder sprake van meer decentralisatie dan verdere centralisatie. Het is moeilijk deze trend in verband te brengen met digitalisering als macrotrend, maar de digitalisering van de manier waarop kerntaken voor de krijgsmacht worden uitgevoerd heeft ontegenzeggelijk voor een dynamiek van decentralisatie gezorgd. De versnippering van veiligheidszorgtaken over actoren die daar lange tijd geen rol en verantwoordelijkheid in hadden -bedrijven en burgers- duidt bovendien ook op meer decentraliteit.

De beantwoording van de deelvragen en de acceptatie van de tweede hypothese betekenen voor de beantwoording van de hoofdvraag dat de noodzaak tot controle van digitale dreigingen tot een meer gedecentraliseerde veiligheidszorg leidt. Deze decentralisatie wordt gekenmerkt door vervlechting en pluraliteit in betrokken actoren. Deze actoren zoeken in opvallende mate toenadering tot elkaar, door in samenwerkingsverbanden en netwerken taken ter bescherming van de nationale veiligheidsbelangen op zich te nemen. Overheidsinstellingen proberen hier als netwerk- en ketenpartner onderdeel van uit te maken door te stimuleren en faciliteren. Deze manier van governance sluit naadloos aan bij de in de bestuurskunde al eerder geconstateerde bestuurlijke paradigmaverschuiving naar *New Public Governance*.

6.2 Implicaties voor vakgebied en aanbevelingen voor vervolgonderzoek

De conclusies en bevindingen uit dit onderzoek hebben enkele implicaties voor de bestuurskunde als wetenschappelijk vakgebied, evenals voor de bestuurlijke praktijk. Ten eerste is besproken dat het gangbare onderscheid tussen interne en externe veiligheid tot het verleden behoort. Dat brengt vragen met zich mee ten aanzien van de instituties die hun oorsprong danken aan dit onderscheid: de krijgs- en politionele macht. Hun relatieve aandeel in de veiligheidszorg neemt af ten gevolge van digitalisering, en de vraag is in hoeverre hun institutionele aard hen in staat stelt effectief om te gaan met de digitalisering van dreigingen. Nieuw wetenschappelijk onderzoek naar effectieve digitale veiligheidszorg kan beleidsmakers voorzien van opties om de traditionele veiligheidsapparaten 'cyberproof' te maken.

Ten tweede leidt digitalisering tot decentralisatie van de veiligheidszorg en vernetwerking van politie, krijgsmacht, bedrijven en burgers. Hier en daar houden wetenschappers zich al bezig met kwesties rondom de mogelijkheden tot burgerbetrokkenheid ten aanzien van digitale veiligheidskwesties[143]. Overheden houden zich ook al in bepaalde mate bezig met sturing van gedrag door burgers en het stellen van voorwaarden aan bedrijven, maar een echte eenkennige lijn ontbreekt nog. Aanvullend wetenschappelijk onderzoek kan hiaten in de kennis hieromtrent vullen, door zich bezig te houden met kwesties omtrent overkoepelende beleidsmogelijkheden om netwerken van burgers, bedrijven en overheden elkaar te laten helpen in de totstandkoming van de veiligheidszorg[144]. Middels publieksonderzoeken, surveys en diepteinterviews kunnen wederzijdse wensen en verwachtingen inzichtelijk gemaakt worden. Inmiddels klinkt ook de roep om meer centrale aansturing hieromtrent, in de vorm van een apart bewindspersoon[145]. Ook de zin hiervan, evenals de mogelijke inrichting hiervan, vragen om vervolgonderzoek.

[143] zie bijvoorbeeld https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93169.pdf

[144] denk bijvoorbeeld aan de mogelijkheden in het stellen van veiligheidsvoorwaarden aan digitale producten (Schneier, 2018)

[145] zie https://www.tweedekamer.nl/downloads/document?id=3b6b4589-3021-4604-a28b-5338757c1959&title=Motie%20van%20het%20lid%20Verhoeven%20c.s.%20over%20het%20instellen%20van%20een%20onderzoekscommissie.pdf

Ten derde nopen de veranderende verhoudingen in de totstandkoming van de veiligheidszorg tot publiek debat omtrent moreelethische overwegingen aangaande het belang van bedrijven en burgers voor de totstandkoming van de veiligheidszorg. Hoe ver mag het gaan? In welke mate is betrokkenheid van bedrijven en burgers verantwoord? In hoeverre mogen andere belangen dan veiligheidsoverwegingen meespelen? Digitalisering als macrotrend lijkt nauwelijks een halt toe te roepen, mocht dat überhaupt wenselijk zijn. Of de mate waarin, en manier waarop actoren ten gevolge van die digitalisering betrokken zijn bij de totstandkoming van publieke diensten te sturen valt, dient onderdeel van beschouwing te zijn. Ten tijde van de Tweede Wereldoorlog stelde Engelberts (1900) voor over te gaan tot 'training van complete natie, opdat volledige natie de krijgsmacht is'. Zo'n tien eeuwen daarvoor werden burgers betrokken middels de *fyrd*. Het is niet gezegd dat digitalisering automatisch tot dergelijke betrokkenheid zal leiden, maar het is wel belangrijk inzicht te hebben in de grenzen die gesteld kunnen (en misschien wel moeten) worden aan de betrokkenheid van bepaalde actoren.

6.2.1 Generaliseren

In hoofdstuk 3 is reeds besproken dat hoewel de interne validiteit van case study research zoals dat hier verricht is doorgaans vrij hoog is, het moeilijk is om onderzoek dat naar enkele cases verricht is te generaliseren naar een grotere populatie. Alle landen ter wereld hebben echter te maken met de huidige macrotrend die digitalisering is. De scheiding tussen interne en externe veiligheid zal voor veel van deze landen ook vervagen, zo niet wegvallen. Het is geen risicovolle aanname dat in landen waarbij eenzelfde digitaliseringstrend onderscheiden kan worden, en waarbij de organisatie van de krijgs- en politionele macht op hoofdlijnen gelijk is aan die in Nederland, de veiligheidszorg ook tekenen van pluralisering en decentralisatie vertoont. Voor landen waarin de samenleving minder intensief digitaliseert, of landen waarin vooral de krijgsmacht verantwoordelijk is voor externe én interne veiligheidszorg, kunnen op basis van het hier verrichte onderzoek geen uitspraken gedaan worden. Hier liggen mogelijkheden voor vervolgonderzoek.

Ten aanzien van de toekomst kunnen nog nauwelijks gefundeerde uitspraken gedaan worden. Met de grootst mogelijke voorzichtigheid zou de verwachting uitgesproken kunnen worden dat als de digitaliseringstrend zich doorzet, de verschillende actoren naar elkaar toe zullen blijven groeien[146] en de veiligheidszorg verder pluraliseert en decentraliseert. Echter, indien de invloed van grote technologiebedrijven blijft toenemen, valt mogelijkerwijs te verwachten dat zij monopolisten ten aanzien van de veiligheidszorg worden. Dit zou een centralisatie van de veiligheidszorg betekenen, maar bij andere actoren dan lange tijd gebruikelijk is geweest.

De constatering dat digitalisering ten gevolge van pluralisering tot decentralisatie leidt, geldt ten aanzien van het geheel aan veiligheidszorg dat geleverd wordt. In dit onderzoek lag de focus op de krijgsmacht, de politionele macht, bedrijven en burgers. Andere actoren zoals de AIVD, MIVD, Marechaussee en de FIOD zijn hier buiten beschouwing gelaten. Allen zijn echter organisaties die in steeds grotere mate gebruik maken van digitale technologieën, zoals als big data. Er kan derhalve verwacht worden dat ook hier specialisatie en dus nood aan autonomie optreedt, evenals grotere afhankelijkheid van technologiebedrijven. Bovendien doet het

[146] zie bijvoorbeeld https://www.trouw.nl/nieuws/leger-en-politie-hebben-elkaar-steeds-harder-nodig~b7fb7d1e/ en het advies van Rood (2014, p.130) om *"samenwerking tussen externe en interne veiligheidsactoren te verdiepen, niet alleen op beleidsniveaus maar ook op de operationele niveaus in de organisatiestructuren"*.

eventuele toevoegen van deze actoren niets af aan de constatering dat bedrijven en burgers in steeds grotere mate medeverantwoordelijk zijn voor de totstandkoming van veiligheidszorg.

6.3 Reflectie

In dit onderzoek is getracht middels methodologische overwegingen (multiple case study reasearch), het opstellen van een gefundeerd toetsingskader en een verscheidenheid aan soorten bronnen zo goed mogelijk inzicht te verkrijgen in de gevolgen die specifiek toe te wijzen zijn aan digitalisering. Deels is dat ook gelukt. Deels echter, blijft het zeer ingewikkeld om digitalisering en de (institutionele, organisationele, bedrijfsmatige en civiele) ontwikkelingen aan elkaar te koppelen. Immers, ook andere ontwikkelingen dragen bij aan het veranderende dreigingsbeeld en de reorganisaties van krijgs- en politionele macht. Desalniettemin is een aantal factoren onderscheiden die in algemene of specifieke zin direct aan digitalisering kunnen worden toegeschreven. Bovendien is als gevolg van de keuze voor kwalitatief onderzoek inzicht verkregen in de manieren waarop de gevonden invloed van digitalisering werkt. Dat kan dienen als opmaat naar aanvullend onderzoek, waarin dit uitgediept en verbreed kan worden.

Ten tweede is het opgestelde toetsingskader voor (de-)centralisatie maar beperkt bruikbaar gebleken. Immers, wetenschappelijke literatuur ten aanzien van (de-)centralisatie en diens indicatoren kent dikwijls een zeer organisationele focus. Bekeken wordt hoe (de-)centraal bepaalde overheidsorganisaties, verenigingen of overige instituties georganiseerd zijn. Digitalisering leidt echter vooral tot vernetwerking; het samenwerken of naar elkaar toe neigen van verschillende organisaties. Voor de analyse hiervan zijn de bekende indicatoren minder geschikt gebleken. Echter, uit vernetwerking en losse samenwerkingsverbanden spreekt impliciet al een grote mate van decentralisatie, waardoor alsnog waardevolle conclusies ten aanzien van de hier gestelde hoofd- en deelvragen konden worden getrokken.

Ten slotte is er in dit onderzoek een sterke focus geweest op perceptie. Immers, de verslechterde veiligheidssituatie waarover gesproken is vooral een gepercipieerde veiligheidssituatie. Er is geen kwantitatieve analyse aan vooraf te gaan om te bepalen in welke mate en nu objectief sprake is van verhoogde onveiligheid. Het is goed verdedigbaar dat digitale technologieën als big data, (semi-)autonome wapensystemen en robotica objectief gezien juist kunnen zorgen voor *verhoogde* veiligheidsniveaus. Anderzijds wijzen verschillende bronnen erop dat slachtofferschap van, en schade door cybercriminaliteit hand over hand toenemen. Naast het feit dat daadwerkelijk objectief inzichtelijk maken hoe de veiligheidssituatie ten gevolg van digitalisering verandert, is gepercipieerde veiligheid een reële factor voor beleid. Immers, het voedt de ‘cyberwapenwedloop’ die zich afspeelt en het beïnvloedt de manier waarop mensen zich gedragen. Ten gevolge van de gepercipieerde verslechterde veiligheidssituatie zijn de verhoudingen ten aanzien van de veiligheidszorg bovendien ingrijpend veranderd.

LITERATUURLIJST

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, *50*(3), 44:1-41.

AIV (2015). Autonome Wapensystemen. De Noodzaak van Betekenisvolle Menselijke Controle. Via: https://aiv-advies.nl/download/3ea81d78-fe71-404c-8aff-62b4898969a7.pdf

Analistennetwerk Nationale Veiligheid (2018). Horizonscan Nationale Veiligheid 2018. Via: https://www.thehaguesecuritydelta.com/media/com_hsd/report/216/document/ANV-Horizonscan-Nationale-Veiligheid-2018.pdf

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Red.), *The economics of information security and privacy* (pp. 265-300). Berlin, Germany: Springer.

Aucoin, P. (1990). Administrative reform in public management: paradigms, principles, paradoxes and pendulums. *Governance, 3*(2), 115-137.

Bantema, W., Twickler, S.M.A., Munneke, S.A.J., Duchateau, M. & Stol, W.Ph. (2018). Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld. Via: https://www.politieenwetenschap.nl/cache/files/5d3996b3ed11ePW103.pdf

Bayley, D. & Shearing, C. (1996). The Future of Policing. *Law and Society Review, 30*(3), 585-606.

Berg, C.E. van den, Stoppelaar, L.M. de, Smits, J.A.H.M.P., Dieters, M.E. & Schonewille, H. (2017). "Ik moet een hoop, maar mag een beetje". De Commandant in zijn kracht. Themaonderzoek IGK 2016. Via: https://www.defensie.nl/binaries/defensie/documenten/rapporten/2017/06/01/themarapport-igk-de-commandant-in-zijn-kracht/170601+themarapport+CIZK+Definitief.pdf

Brennen, J. S., & Kreiss, D. (2016). Digitalization. *The international encyclopedia of communication theory and philosophy*, 1-11.

Brenner, S. W. (2014). *Cyberthreats and the Decline of the Nation-State*. London, UK: Routledge.

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. New York, NY, US: W W Norton & Co.

Cachet, A. & Prins, R. (2012). Ontwikkeling van het lokaal veiligheidsbeleid. In: E. Muller (Red.) *Veiligheid en veiligheidsbeleid in Nederland*. Alphen aan de Rijn, Nederland: Kluwer.

Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101-114.

Clingendael (2018). Interrregnum. Strategische Monitor 2018-2019. Via: https://www.clingendael.org/sites/default/files/2019-04/stratmon-2018-2019-interregnum-nl.pdf

Cornelisse, L. (2011). Dubbele ramp. Via:

https://www.ifv.nl/kennisplein/Documents/binnenlandsbestuur-nr-1-januari-2011-dubbele-ramp.pdf

Creveld, M. L. van, (1999). *The rise and decline of the state*. Cambridge, UK: Cambridge university press.

Cusumano, E. & Corbe, M. (2018). A civil-military response to hybrid threats. Via: https://link.springer.com/content/pdf/10.1007%2F978-3-319-60798-6.pdf

Das, D., Huberts, L., & van Steden, R. (2007). The changing "soul" of Dutch policing: Responses to new security demands and the relationship with Dutch tradition. *Policing: An International Journal of Police Strategies & Management*, *30*(3), 518-532.

Dempsey, J. S., & Forst, L. S. (2012). *An introduction to policing*. Boston, MA, US: Cengage Learning.

Donahue, A. K., Eckel, C. C., & Wilson, R. K. (2014). Ready or not? How citizens and public officials perceive risk and preparedness. *The American Review of Public Administration*, *44*(4), 89S-111S.

Dunlap Jr, C. J. (1999). The police-ization of the military. *Journal of Political & Military Sociology*, *27*(Winter), 217.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—long live digital-era governance. *Journal of public administration research and theory*, *16*(3), 467-494.

Eeten, M. van, Asghari, H., Bauer, J. M., & Tabatabaie, S. *Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market.* The Hague, Netherlands: Ministry of Economic Affairs, 2011.

Engelberts, W.M. (1900). *De reorganisatie onzer landmacht*. Amsterdam, Nederland: L.J. Veen.

Europol (2019). European Union Terrorism Situation and Trend Report 2019. Via https://www.europol.europa.eu/sites/default/files/documents/tesat_2019_final.pdf

Fijnaut, CJ. C. F. (1979). *Opdat de macht een toevlucht zij? Een historische studie van het politieapparaat als een politieke instelling*. Antwerpen, België: Kluwer Rechtswetenschappen.

Gallie, W. B. (1956). Essentially contested concepts. *Proceedings of the Aristotelian society* (56), 167-198.

George, A. L., & Smoke, R. (1974). *Deterrence in American foreign policy: Theory and practice*. Columbia University Press.

Gerring, J. (2007). *Case Study Reasearch. Principles and Practises*. New York, US: Cambridge.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-606.

Gruening, G. (2001). Origin and theoretical basis of New Public Management. *International public management journal*, *4*(1), 1-25.

Hakvoort, J.L.M. (1995). *Methoden en Technieken van Bestuurskundig Onderzoek*. Delft,

Nederland: Eburon.

Harvey, D. (2007). *A brief history of neoliberalism*. Oxford, USA: Oxford University Press.

Hebenton, B. en Thomas, T. (1995). *Policing Europe: Co-operation, Conflict and Control.* New York, US: Palgrave

Helsloot, I., Pieterman, R., & Hanekamp, J. C. (2010). *Risico's en redelijkheid*. Den Haag, Nederland: Boom Juridische uitgevers.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Heywood, A. (2017). *Political ideologies: An introduction*. Macmillan International Higher Education.

Hood, C. (1991). A public management for all seasons? *Public administration*, *69*(1), 3-19.

Howard, M. (2006). *War in European history.* Oxford University Press.

Hutchcroft, P. D. (2001). Centralization and decentralization in administration and politics: assessing territorial dimensions of authority and power. *Governance*, *14*(1), 23-53.

Hyndman, N., & Liguori, M. (2016). Public sector reforms: Changing contours on an NPM landscape. *Financial Accountability & Management*, *32*(1), 5-32.

Instituut Fysieke Veiligheid (2018). Maatschappelijke onrust en de rol van gemeenten. Een inventariserend onderzoek. Via: https://www.ifv.nl/kennisplein/Documents/20180416-IFV-Maatschappelijke-onrust-en-de-rol-van-gemeenten.pdf

Jansen, J. (2016). Linksom of rechtsom. Over (de) centralisering in de veiligheidszorg. *Proces*, *95*(3), 37-47.

Jinks, D. (2003). State responsibility for the acts of private armed groups. *Chi. J. Int'l L.*, (*4)*83.

Jones, T., & Newburn, T. (2002). The transformation of policing? Understanding current trends in policing systems. *The British journal of criminology, 42*(1), 129-146.

Kääriäinen, J., & Sirén, R. (2012). Do the police trust in citizens? European comparisons. *European Journal of Criminology*, *9*(3), 276-289.

Keren, M., & Levhari, D. (1989). Decentralization, aggregation, control loss and costs in a hierarchical model of the firm. *Journal of Economic Behavior & Organization*, *11*(2), 213-236.

Knapen, P. (2017) Burgerparticipatie bij Team High Tech Crime. Wat zijn de mogelijkheden en Kansen voor de toekomst? Via: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93169.pdf

Koopman, J. (2013). [Review van het boek *Het nationale politiekorps: achtergronden, controverses en toekomstplannen*, door C.J.F.J. Fijnaut]. *TvCR,* 2013:1.

KPMG (2009) 'Feasibility Studies naar de PIOFACH taken van de Politie Deel 1'. Via: http://www.tweedekamer.nl/downloads/document?id=00f8b0b0-e959-4050-9829-81261309fa4d&title=Eindrapportage%20Feasibility%20Studies%20naar%20de%20PIO

Kuijken, W.J., Gortzak, P.J., 't Hart, P., Leeuw, F.L., Sorgdrager, W., Thiel, S. van & Uhm, P.J.M. van (2017) Evaluatie Politiewet 2012. Doorontwikkelen en Verbeteren. Via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/11/16/evaluatie-politiewet-2012-doorontwikkelen-en-verbeteren/EK+Bijlage1+Evaluatie+Politiewet+2012+Doorontwikkelen+en+verbeteren.pdf

Leander, A. (2005). The power to construct international security: On the significance of private military companies. *Millennium*, *33*(3), 803-825.

Li, M., Chen, J., Chen, T., & Yuan, H. (2010). Probability for disaster chains in emergencies. *Journal of Tsinghua University Science and Technology*, *50*(8), 1173-1177.

Lipsky, M. (2010). *Street-level bureaucracy: Dilemmas of the individual in public service*. Russell Sage Foundation.

Lone, Q., Moura, G. C., & Van Eeten, M. (2014). Towards incentivizing ISPs to mitigate botnets. In *IFIP International Conference on Autonomous Infrastructure, Management and Security* (pp. 57-62). Springer, Berlin, Heidelberg.

Mann, M. (1993). *The sources of social power: Volume 2, the rise of classes and nation-states, 1760-1914* (Vol. 2). Cambridge University Press.

Meijer, A.J., Grimmelikhuijsen, S.G., Fictorie, D., Thaens, M. & Siep, P. (2013). Politie & sociale media. Van hype naar onderbouwde keuzen. Reed Business Information.

Meulen, N. van der (2013). DigiNotar: Dissecting the first dutch digital disaster. *Journal of Strategic Security*, *6*(2), 46-58.

Ministerie van Buitenlandse Zaken (2018). Wereldwijd voor een veilig Nederland. Geintegreerde Buitenland- en Veiligheidsstrategie 2018-2022. Via https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

Ministerie van Defensie (2018). Defensienota 2018. Investeren in onze mensen, slagkracht en zichtbaarheid. Via: https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2018/03/26/defensienota-2018/210318+Defensienota+definitief.pdf

Ministerie van Justitie en Veiligheid (2018). Kamerbrief over de evaluatie politiewet 2012. Via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/06/15/kamerbrief-over-de-evaluatie-politiewet-2012/kamerbrief-over-de-evaluatie-politiewet-2012.pdf

NCTV (2013). Nationale Cyber Security Strategie 2. Via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf

NCTV, (2016). Nationaal Veiligheidsprofiel 2016. Via:

https://www.nctv.nl/binaries/Nationaal%20Veiligheidsprofiel%202016_tcm31-232083.pdf

NCTV (2018a). Nederlandse Cyber Security Agenda: Nederland digitaal veilig. Via: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf

NCTV (2018b) Cyber Security Beeld Nederland. Via: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2018/1/CSBN_2018.pdf

NCTV (2019a). Dreigingsbeeld Terrorisme Nederland 50. Via: https://www.nctv.nl/binaries/DTN50%20samenvatting_tcm31-395216.pdf

NCTV (2019b). Nationale Veiligheid Strategie 2019. Via: https://www.nctv.nl/binaries/Nationale%20Veiligheid%20Strategie%202019_tcm31-393099.pdf

NCTV (2019c). Risico- en Crisisbarometer Voorjaar 2019. Via: https://www.nctv.nl/binaries/B4277%20NCTV%20Risico%20en%20Crisisbarometer%20voorjaar%202019_tcm31-387080.pdf

Osborne, S.P., (2006) The new public governance? Public Management Review, 8, 377-388.

Osborne, S. P. (Ed.). (2010). *The new public governance: Emerging perspectives on the theory and practice of public governance*. Routledge.

Osiel, M. J. (1988). *Obeying orders: atrocity, military discipline and the law of war*. Routledge.

Pestoff, V. (2018) Co-Production at the Crossroads of Public Administration Regimes. In Brandsen, Steen & Pestoff (Reds.). *Co-Production and Co-Creation. Engaging Citizens in Public Services*. Routledge, New York.

Phelps, M. L. (2014). Doppelgangers of the State: Private Security and Transferable Legitimacy. *Politics & Policy*, *42*(6), 824-849.

Pieterman, R. (2008). *De voorzorgcultuur: streven naar veiligheid in een wereld vol risico en onzekerheid*. Boom Juridische Uitgevers.

Reiss Jr, A. J. (1992). Police organization in the twentieth century. *Crime and Justice*, *15*, 51-97.

Rid, T. (2012) Cyber War Will Not Take Place, Journal of Strategic Studies, 35:1, 5-32,

Rood, J. (2014). Een wankele wereldorde. Clingendael Strategische Monitor 2014. Via: https://www.clingendael.org/sites/default/files/pdfs/Clingendael_strategische_monitor_2014_Een_wankele_wereldorde_0.pdf

Rynck, F. de & Wayenberg, E. (2013) De lokale besturen. In: Hondeghem, Van Dooren, De Rynck, Verschuere en Op de Beeck (Reds.) Handbook Bestuurskunde. Via: https://biblio.ugent.be/publication/8572129/file/8572147

Shackelford, S. (2018). 30 Years Ago, The World's First Cyberattack Set The Stage For Modern

Cybersecurity Challenges. Via: http://cyberlaw.stanford.edu/publications/30-years-ago-worlds-first-cyberattack-set-stage-modern-cybersecurity-challenges

Schneider, A. (2003). Decentralization: Conceptualization and measurement. *Studies in comparative international development*, *38*(3), 32-56.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Schwab, K., & Davis, N. (2018). *Shaping the future of the fourth industrial revolution*. Currency.

Shaw, W. L. (1961). Selective Service: A Source of Military Manpower. *Mil. L. Rev.*, *13*, 35.

Shearing, C. D., & Stenning, P. C. (1983). Private security: implications for social control. *Social problems*, *30*(5), 493-506.

Slijper, F., Beck, A., Kayser, D. & Beenes, M. (2019a). Don't be evil? A survey of the Tech Sector's stance on lethal autonomous weapons. Via: https://www.paxforpeace.nl/media/files/pax-report-killer-robots-dont-be-evil.pdf

Slijper, F., Beck, A. & Kayser, D. (2019b). State of AI. Artificial Intelligence, the military and increasingly autonomous weapons. Via: https://www.paxforpeace.nl/media/files/state-of-artificial-intelligence--pax-report.pdf

Smits, M. & Besters, M. (2011). Politierobots in Nederland: zegen of dreiging voor de veiligheid van burgers? Via: https://martijntje.nl/media/files/Politie_robots_hoofdstuk_DEFINITIEF1sep_2011.pdf

Stead, P.J. (1957). *The Police of Paris.* London: Staples.

Sterling, C. (2008). *Military communications : From ancient times to the 21st century*. Santa Barbara, California: ABC-CLIO.

Terpstra, J.B. en Gunther Moor, L. (2012). Nationale Politie. Kanttekeningen tegen de stroom in. Via: https://repository.ubn.ru.nl/bitstream/handle/2066/142568/142568.pdf

Terpstra, J. B., Foekens, P. W., & van Stokkom, B. A. M. (2015). Burgemeesters over hun nationale politie. Via: https://repository.ubn.ru.nl/bitstream/handle/2066/141809/141809.pdf

Terpstra, J. B., & van Stokkom, B. A. M. (2015). Politie in tweevoud: centraal en decentraal. Een analyse van enkele achtergronden en spanningen.

Terpstra, J. B., & Vijver, K. (2005). Het Nederlands politiebestel en de druk tot centralisatie. Via: https://repository.ubn.ru.nl/bitstream/handle/2066/128951/128951.pdf?sequence=1

Treur, J. H. F. (1998). *Centralisatie en decentralisatie bij de Nederlandse politie. Over actuele aansturing en resultaatverantwoordelijkstelling bij de Nederlandse politie*. Groningen: Koninklijke Vermande.

Toms, V. (2018). Digitale Hygiëne Nederland. Via: https://www.dcypher.nl/sites/default/files/uploads/documents/Rapport%20_Digitale%20Hygiene%20Nederland%20-%20Juni%202018_.pdf

Tsirigotis, A. (2017). *Cybernetics, warfare and discourse : The cybernetisation of warfare in britain*. Cham, Switzerland: Palgrave MacMillan.

Värk, R. (2017). Declared and Undeclared Wars. *Journal on Baltic Security*, *3*(1), 25-31.

Vedung, E. (2015). Autonomy and street-level bureaucrats' coping strategies. Nordic Journal of Studies in Educational Policy, 2015(2), 28643.

Verbond van Verzekeraars (2018). Cybercriminaliteit. Via: https://www.verzekeraars.nl/verzekeringsthemas/nieuwe-risicos/cybercriminaliteit

Vijver, C.D. van der, Meershoek, A.J. & Slobbe, D. (2001). Kerntaken van de politie. Een inventarisatie van heersende opvattingen. Zeist: Kerckebosch.

Vries, P.H. de, (2015). Discipline. Via: https://www.militairespectator.nl/thema/ethiek/gastcolumn/discipline

Waard, E.J. de, (2011). De Nederlandse expeditionaire krijgsmacht: Slim en slagvaardig?. *Militaire spectator*, *180*(5), 214-223.

Wagenaar, F. (1997). *"dat de regeringe niet en bestaet bij het corpus van de magistraet van Den Hage alleen" : De sociëteit van 's-gravenhage (1587-1802) : Een onderzoek naar bureaucratisering* (Doctoral dissertation, 1997). S.n.

Wal, R. van der (2004). Het leger: hoeder van de openbare orde en veiligheid in de negentiende eeuw. Militaire spectator, 173-2.

Weger, M. de (2006). *De binnenlandse veiligheidstaken van de Nederlandse krijgsmacht.* Van Gorcum.

Wintle, M. (1996). Policing the liberal state in the Netherlands: the historical context of the current reorganization of the Dutch police. *Policing and Society: An International Journal*, *6*(3), 181-197.

World Economic Forum (2018). The Global Risks Report 2018. 13th Edition. Via: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Wright, Q. (1932). When does war exist? *American Journal of International Law*, *26*(2), 362-368.

WRR (2017a). Veiligheid in een wereld van verbindingen: Een strategische visie op het defensiebeleid. Via: https://www.wrr.nl/binaries/wrr/documenten/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen/R098-Veiligheid-in-een-wereld-van-verbindingen.pdf

WRR (2017b). *Weten is nog geen doen. Een realistisch perspectief op redzaamheid.* Via: https://www.wrr.nl/binaries/wrr/documenten/rapporten/2017/04/24/weten-is-nog-geen-doen/R097-Weten-is-nog-geen-doen.pdf