Universiteit Utrecht

USBO
advies

Op weg naar een Weerbare Open Samenleving

Bouwstenen voor een toekomstvisie

definitief

November 2018

Op weg naar een Weerbare Open Samenleving

Bouwstenen voor een toekomstvisie

In opdracht van het WODC

Kernteam:
Prof. dr Mirko Noordegraaf (projectleider)
Dr Marie-Jeanne Schiffelers (uitvoerend projectleider)
Dr Karin Geuijen
Dr Paulien de Morree
Prof. dr Jacco Pekelder

Expertteam:
Prof. dr Kees van den Bos
Prof. dr Beatrice de Graaf
Prof. dr Paul 't Hart
Prof. dr Henk Kummeling

Eindrapport November 2018

COLOFON

Titel:	Op weg naar een Weerbare Open Samenleving
Auteurs:	Mirko Noordegraaf, Marie-Jeanne Schiffelers, Karin Geuijen, Paulien de Morree, Jacco Pekelder
Studentassistent:	Esther Leferink
Opdrachtgever:	Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid
	Utrecht, November 2018

Samenvatting

Op weg naar een Weerbare Open Samenleving

Achtergrond en vraagstelling

Veiligheidsdenken heeft in westerse samenlevingen stevig postgevat. Dreigingen dienen zich in snel veranderende en steeds complexere vorm aan. De overheid stelt zichzelf de opgave om de (vaak nog niet bekende) risico's te beteugelen, *'taming of the future'* (De Graaf, 2013). Zij doen dit door de weerbaarheid van de samenleving tegen deze dreigingen te verhogen en er op zo gepast mogelijke en gecoördineerde wijze mee om te gaan met de continue inachtneming van de onderliggende waarden van onze democratische rechtsstaat.

Doel van dit onderzoek is het aanleveren van *bouwstenen* voor de discussie over de omgang met complexe veiligheidsuitdagingen waar de Nederlandse samenleving en overheid zich voor gesteld zien. Meer specifiek zoeken we naar voorbeelden die laten zien welke veiligheidspraktijken ingezet worden om op (potentiële) dreigingen te anticiperen en reageren, hoe dat gebeurt en door wie. We kijken daarbij vooral naar hoe deze praktijken zich verhouden tot de belangen die verdedigd dienen te worden. Daarvoor hanteren wij het concept van de weerbare open samenleving (WOS). Kunnen overheden een *balans* vinden tussen enerzijds het weerbaar maken van een samenleving en anderzijds het beschermen van de open samenleving met inachtneming van democratische en rechtsstatelijke waarden? De hoofdvraag die wij in dit onderzoek hanteren luidt:

- *Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?*

Deze hoofdvraag is om redenen van onderzoekbaarheid teruggebracht naar het uitwerken van twee specifieke verstoringen/dreigingen in andere landen die naar verwachting van belang zijn voor de Nederlandse context. Daartoe is een tweetal *experienced cases* beschreven van westerse democratieën en hun omgang met een complexe, grensoverschrijdende dreiging/verstoring. Doel van de casuïstiek is het ophalen van mogelijke lessen ten behoeve van de Nederlandse aanpak. In dit onderzoek is gekozen voor de volgende twee casus:

- *Duitsland*: Omgaan met migrantenstromen
- *Israël*: Afwending van *cyber*aanvallen

De Duitse casus is interessant vanwege zijn (initiële) openheid in de opvang van de grootschalige migrantenstroom die Duitsland als eindbestemming koos. In het recordjaar 2015 ving Duitsland meer dan 2,1 miljoen migranten op, bijna een verdrievoudiging van de hoeveelheid migranten die Duitsland in 2010 (0,8 miljoen) welkom heette (Das Statistik Portal, 2017). De Duitse regering lijkt in samenwerking met regionale overheden en publieke en non-profit organisaties, goed in te kunnen spelen op deze migrantenstroom. De gekozen insteek leidt echter ook tot grote weerstand bij delen van de bevolking en de politiek en zet daarmee de openheid en mogelijk ook de weerbaarheid van de samenleving onder druk.

De Israëlische casus is interessant vanwege de hoge weerbaarheid ten opzichte van *cybercrime*. Geen enkele ander natie heeft het afgelopen decennium zoveel geïnvesteerd in *cybersecurity*. De Israëlische overheid en het Israëlische bedrijfsleven exporteren zelfs op grote schaal kennis en technische middelen naar andere landen om *cyber*aanvallen te herkennen en af te wenden (Forbes, 2017). De keuze voor deze casus betekent echter niet dat Israel weerbaarheid op een voor Nederland wenselijke wijze combineert met democratische en rechtsstatelijke waarden. Israel laat volgens onder meer diverse internationale als Israëlische mensenrechten organisaties met regelmaat een beeld zien waarbij de democratische en rechtsstatelijke waarden onder druk staan. Deze casus geeft dan ook vooral inzicht in de mogelijke voor en nadelen van dit type veiligheidspraktijken in termen van een weerbare open samenleving.

De hoofdvraag van dit onderzoek is beantwoord door middel van een *multidisciplinair* onderzoek, waarbij de problematiek vanuit de disciplines bestuurs- en organisatiewetenschap, rechtsgeleerdheid en geschiedenis is bestudeerd. Voor de beantwoording van de onderzoeksvragen is gebruik gemaakt van verschillende onderzoeksmethoden waarbij literatuurstudie en expertinterviews de basis vormen. De casuïstiek is uitgewerkt, gebruikmakend van geschreven bronnen en expertinterviews. Vervolgens zijn de bevindingen uit de casuïstiek tegen het licht van de Nederlandse context bezien. Hiervoor is wederom gebruik gemaakt van geschreven bronnen en expertinterviews.

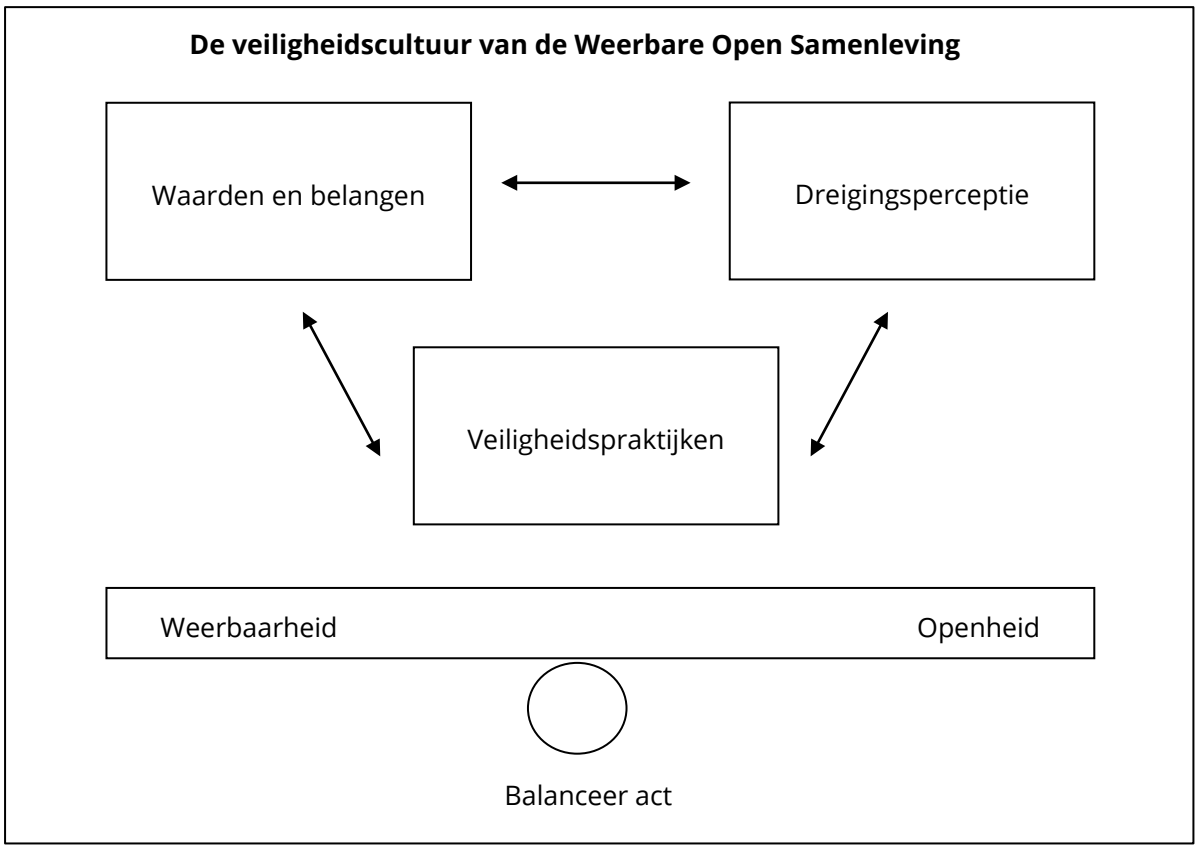
Analysekader

In dit onderzoek kijken we naar de veiligheidscultuur van samenlevingen die *tegelijkertijd* weerbaar en open willen zijn. Dat vraagt om een continue 'balanceer act' tussen twee grootheden die elkaar kunnen versterken maar elkaar ook kunnen ondermijnen. De Graaf (2014, p.7) formuleerde drie vragen om de veiligheidscultuur voor een specifieke situatie te beschrijven:

1 Welke waarden en belangen vinden wij beschermwaardig?
2 Wie en/of wat zien wij als potentiële dreigingen?
3 In welke veiligheidspraktijken vertaalt zich dat?

Deze conceptualisering van de 'veiligheidscultuur' dient als theoretische drieslag in de verschillende hoofdstukken. Dat wil zeggen dat we ons in dit onderzoek richten op deze drie deelvragen en het samenspel daartussen binnen de context van een weerbare open samenleving. We inventariseren wat dit samenspel ons leert over de wijze waarop in een specifieke context wordt omgegaan met een specifieke grensoverschrijdende dreiging en wat Nederland van die werkwijze kan leren. Dit wordt telkens gekoppeld aan de afwegingen die gemaakt worden tussen openheid en weerbaarheid. In onderstaande figuur 1 wordt dit gevisualiseerd.

Figuur 1. Analysekader



Aan de hand van de landencasuïstiek is gezocht naar antwoorden op de volgende deelvragen:

1 *Welke dreiging zien deskundigen in de betreffende landen rondom de gekozen thematiek voor de weerbare open samenleving? Welke waarden en belangen zijn daarbij beschermwaardig?*
2 *Welke praktijken worden gehanteerd om deze dreigingen het hoofd te bieden:*
   a *Welke mogelijkheden zien deskundigen in de betreffende landen om met technologische middelen of anderszins, disruptieve maatschappelijke ontwikkelingen in een vroegtijdig stadium te voorzien?*
   b *Wat is de uitvoerbaarheid van deze maatregelen?*
   c *Welke gevolgen hebben de snelle veranderingen van de dreigingen voor de (interne) organisatie van zowel private als publieke betrokken partijen en wat betekent dit voor de benodigde capaciteit*[1]*?*
   d *In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?*
3 *Welke mogelijke gevolgen hebben de ingezette praktijken voor de weerbare open samenleving?*

Bevindingen: Duitsland en het migratievraagstuk

Dit onderzoek laat zien dat de vluchtelingencrisis in Duitsland in zeer sterke mate een *legitimiteitscrisis* is geworden voor het bestaande bestuurlijke bestel. Diverse ontwikkelingen zoals het chaotische opvangbeleid in de nazomer in herfst van 2015, het niet in staat zijn de grenzen te controleren, diverse incidenten en aanslagen, het toenemend extremisme van rechter- én linkerzijde leidden tot verlies van vertrouwen in de gevestigde leiders en partijen en de overheidsorganen. Dit heeft tot gevolg dat Duitsland te maken krijgt met een groeiende polarisatie in de samenleving rond het thema asiel en migratie, een polarisatie die een aantasting betekent van de consensuele orde van de Bondsrepubliek en de maatschappelijke cohesie en het onderling vertrouwen van de burgers in elkaar ondermijnt.

In de omgang met de aan migratie gekoppelde veiligheidsproblemen (met name van terrorisme) heeft de Duitse overheid hoge verwachtingen van de inrichting van nieuwe IT-systemen. Een belangrijk voorbeeld bleek de inrichting van de nieuwe omvattende IT-architectuur, Polizei 2020. De verwachting is dat die technologische maatregelen het vroegtijdig signaleren en analytisch in kaart brengen van veiligheidsrisico's mogelijk maken, en dat betrokken organisaties en individuen daarmee gerichter aangepakt kunnen worden. Daarnaast is er veel aandacht voor het coördineren van de werkzaamheden van verschillende politie- en veiligheidsdiensten en de bij migratie betrokken diensten en voor het informeren van politiek en publiek over de ontwikkelingen met als doel een genuanceerder en feitelijker debat.

Het onder regie van het Bundeskriminalamt (BKA) verzamelen van essentiële informatie door de belangrijkste overheidsorganen op het terrein van migratie en veiligheid en het onderling delen ervan heeft verder een goed *platform* gecreëerd voor 1) de signalering en 2) de bestrijding van migratie-gerelateerde criminaliteit en 3) de communicatie daarover met politiek en publiek.

---

[1] De term "capaciteit" wordt breed opgevat. Het kan gaan over in te zetten mankracht, materieel, maar ook over voldoende (beleids)maatregelen/instrumenten om een bepaalde dreiging aan te pakken.

De verbeterde informatiepositie en de intensievere communicatie zijn echter relatief laat op gang gekomen. Bovendien is hier nog winst te behalen. Verder is ingezet op de sterkere betrokkenheid van niet primair op veiligheid gerichte overheidsdiensten zoals de migratiedienst BAMF bij die nieuwe centrale IT-systemen. Daarmee wordt ingezet op grotere mate van bewustzijn binnen de brede overheid voor veiligheidsaspecten van het specifieke taakgebied.

Er is volgens diverse respondenten in Duitsland sinds 2015 veel politieke en bestuurlijke wil aanwezig bij de verschillende diensten om zich gezamenlijk in te zetten voor de uitvoering van de voorgenomen maatregelen. Men ziet zich gezamenlijk voor de taak gesteld om het aangetaste vertrouwen in de overheid van grote delen van de bevolking en daarmee de legitimiteit van de overheid te herstellen. Tegelijkertijd wordt de politieke en bestuurlijk daadkracht op de proef gesteld door een partij als de AfD en andere populistische krachten, met name ter rechterzijde. Daarnaast wijzen alle gesprekspartners op het Duitse federalisme als een factor die de benodigde samenwerking en afstemming onder druk zet, omdat de deelstaten toch blijven hechten aan de eigen competenties.

Qua capaciteit is er ook nog een flinke weg te gaan. Voor 2015 is er in Duitsland jarenlang bezuinigd op met name de politie en de migratiedienst en de prijs daarvan werd duidelijk gevoeld. De grote toestroom van vluchtelingen stelde de betrokken diensten dan ook voor een groot capaciteitsprobleem in termen van mensen en middelen. Sinds 2015 is er meer budget en meer personeel toegewezen aan de betrokken diensten om te kunnen omgaan met de veiligheidsaspecten gekoppeld aan de vluchtelingencrisis, maar de middelen zijn volgens de respondenten nog ver van toereikend. Wel worden de beschikbare capaciteiten beter geclusterd. Zo heeft het BKA een meer centrale rol gekregen in de verzameling en analyse van gegevens van nieuwkomers.

Er is in Duitsland tegelijkertijd een duidelijke onderstroom van openheid voor migranten die tot uitdrukking komt in vele burgerinitiatieven, zoals het Augsburgse Grandhotel Cosmopolis, en in vele initiatieven en stellingnames uit het bedrijfsleven. Er zijn vele leertrajecten en vacatures voor asielzoekers en andere migranten geopend en in het Duitse asieltraject is ook een vaste rol voor het arbeidsbureau weggelegd. Relatief veel asielzoekers, ook uit de stroom van 2015, hebben inmiddels werk gevonden. Deze onderstroom draagt in potentie op de lange duur veel bij aan de oplossing van het migratie- en integratievraagstuk en is daardoor indirect van belang voor het versterken van de weerbaarheid van de open samenleving. Ze is ook een mogelijke bron van inspiratie voor Nederland.

Kijken we naar de balanceer act tussen veiligheid en openheid als het wezen van de weerbare open samenleving dan vergt dat een voortdurende reflectie op het optreden van betrokken overheidsdiensten. In Duitsland is het overheidsoptreden sterk ingekaderd in de FDGO (Freiheitliche Demokratische Grundordnung: een serie grondwetsartikelen die de Duitse waarden samenvatten). De FDGO biedt een nagenoeg onomstreden richtinggevend kader voor alle beleid.

Bestuurders lijken er mede daardoor van doordrongen te zijn dat veiligheidsmaatregelen ten koste kunnen gaan van de openheid van de Duitse samenleving. Tegelijkertijd heeft de aanscherping van het asielrecht en andere wetgeving, deels in antwoord op de grotere gepercipieerde dreiging door onder meer de Gefährder (bedreigers), geleid tot een verscherping van de politie- en detentiepraktijk. De openheid van de Duitse samenleving komt hiermee onder druk te staan.

Bevindingen: Israël en het *cyber*vraagstuk

Uit ons onderzoek komt naar voren dat de bedreigingen van de *cybersecurity* (*cybercrime*, *cyber*terrorisme, *cyber*spionage) in Israël sterk gelinkt worden aan de algemene veiligheid van het land. De dreigingsperceptie is een dominante en constante factor in de veiligheidscultuur. Deze dominante dreigingsperceptie vormt, samen met de economische belangen op het vlak van *cybersecurity*, de katalysator voor een sterke gerichtheid op (het investeren in) weerbaarheid. Digitale weerbaarheid is gericht op de vitale infrastructuren, maar ook steeds meer op overheidsinstellingen en bedrijven die hun weerbaarheid op orde moeten hebben. De Israëlische overheid is hierbij sterk sturend. Daarnaast speelt het leger een belangrijke rol in ontwikkeling kennis en producten en sterke veiligheidsdenken in Israël. Daar komen *signaleren* en *innoveren* bij elkaar.

In Israël is sprake van een grote mate van bewustzijn voor mogelijke dreigingen voor de *cyber*security. Dit bewustzijn wordt zowel in het leger als in het reguliere onderwijs gecreëerd. Verder wordt door de overheid veel geïnvesteerd in innovatiekracht via start ups en *Cybercenters* en wordt er intensief samengewerkt tussen private en publieke partijen op het gebied van *cybersecurity*. De investeringen en samenwerkingen zijn gericht op kennisuitwisseling tussen de diverse organisaties. Hoewel Israël veel investeert in *cybersecurity* blijkt men ook hier te kampen met een tekort aan goede *cyber*experts. De sterke samenwerking triple helix (overheid, universiteiten, bedrijfsleven) met sterk onderling vertrouwen en makkelijke uitwisseling van capaciteit, kennis en expertise biedt hier slechts ten dele een oplossing voor.

Er is geen helder zicht verkregen op welke specifieke onderdelen publieke organisaties ten aanzien van *cybersecurity* kunnen leren van de private ondernemingen. Wel is duidelijk dat het bedrijfsleven sterk gericht is op innovatie en dat de Israëlische *start up* cultuur een grote innovatiekracht met zich meebrengt. Waar wellicht vooral van te leren is, is de mate van bereidheid van de overheid om te investeren in de onderzoekscentra en de relatief soepele roulatie van personeel en de (daaraan gekoppelde) uitwisseling van kennis en tussen verschillende organisaties.

Weerbaarheid vereist nauwe samenwerking en intensieve kennisuitwisseling met het bedrijfsleven maar de relatie overheid/bedrijfsleven is delicaat. De Israëlische overheid wil graag bedrijven aantrekken vanuit economisch perspectief en vanuit het perspectief van innovatiekracht ten behoeve van de weerbaarheid. Tevens wil de overheid stevig grip hebben op het bedrijfsleven. Het voornemen van de Israëlsiche overheid, om zich via een nieuw wetsvoorstel meer bevoegdheden toe te eigenen en toe te werken naar centralistische vorm van sturing, leidt tot weerstand bij

onder meer het bedrijfsleven maar ook bij mensenrechtenorganisaties die zich zorgen maken om de effecten ervan op onder meer de privacy.
Kijken we naar de Israëlische casus in termen van de weerbare open samenleving dan wordt als snel duidelijk dat de dominante dreigingsperceptie de katalysator vormt voor een sterke gerichtheid op (het investeren in) weerbaarheid en daarmee in *cybersecurity* maatregelen. Het leidt ook tot de sterke neiging tot centralistisch gestuurde controle door de overheid. De sterke gerichtheid op *cybersecurity* maatregelen maakt dat andere belangen in het gedrang komen. Zaken als privacy, burgerrechten, rechtsstatelijke en democratische checks en balances staan duidelijk minder hoog op de agenda. Dit heeft mogelijke gevolgen voor het waarborgen van de privacy van burgers, voor bedrijfsbelangen, voor de balans tussen effectief optreden en rechterlijke en parlementaire controle, en voor interbestuurlijk toezicht.

Vertaling naar Nederland

1 *Wat kan Nederland leren van de betreffende landenpraktijken voor de inzet van maatregelen voor de weerbare open samenleving?*
2 *Wat kunnen de snel veranderende problematieken/dreigingen rondom onder meer asiel- en migratieproblematiek en cybersecurity betekenen voor (afstemming tussen) werkprocessen van Nederlandse (overheids)organisaties die verantwoordelijk zijn voor het Nederlandse veiligheidsbeleid onder meer als het gaat om agendering en besluitvorming en welke capaciteiten, zowel kwantitatief als kwalitatief (competenties) zijn nodig om de weerbaarheid van de Nederlandse overheidsorganisaties te versterken?*

In Nederland is een aantal belangrijke bouwstenen voor veerkrachtig omgaan met verstoringen in vluchtelingenkwesties al goed aanwezig. Zo is er sprake van goed functionerende netwerken van cruciale organisaties. Er wordt veel informatie uitgewisseld, in toenemende mate lukt dat ook internationaal en over sectoren heen. Ook is veel ingezet op (publieks)communicatie waarmee transparantie over beleidskeuzes en veiligheidspraktijken wordt bevorderd. Dit kan bijdragen aan het tegengaan van ‘feitenvrije’ c.q. ‘feitenloze’ debatten die aanleiding kunnen geven tot polarisatie en tot ongefundeerde zorg die het draagvlak kunnen aantasten.

We constateren op basis van dit onderzoek dat Nederland twee bouwstenen kan gebruiken uit de Duitse casus voor het verder versterken van de weerbaarheid en openheid op het terrein van omgaan met vluchtelingenkwesties. De eerste is het explicieter in de (dagelijkse) veiligheidspraktijken reflecteren op *fundamentele principes* als mensenrechten, privacy, en persoonlijke integriteit. De Nederlandse prakijken zijn ‘pragmatisch’, in de zin van daadkrachtig, effectief en efficiënt. Het is belangrijk om naast het verder uitbouwen en versterken van deze *instrumentele* kant ook voortdurend bewust te reflecteren op de *principiële* aspecten van het handelen als professionals in de betrokken organisaties. De tweede bouwsteen gaat over de rol van *publiek-private partnerschappen* in het versterken van weerbaarheid en veerkracht van de samenleving.

Ook dit is een aspect dat in de Nederlandse situatie al bestaat, maar dat kan verder versterkt worden. Dat vereist het creëren van ruimte voor en het faciliteren van burgerinitiatieven alsmede initiatieven door het bedrijfsleven in het laten participeren van asielzoekers. De overheid hoeft daarin lang niet altijd een leidende rol te spelen maar kan dit wel stimuleren.

Waar we met betrekking tot het asiel- en migratievraagstuk het gevaar zien dat dit wellicht te snel gekoppeld wordt aan dreigingen voor de samenleving, zien we bij *cyber*gerelateerde dreigingen eerder een omgekeerd gevaar, namelijk dat er in de Nederlandse maatschappij nog onvoldoende bewustzijn is voor de dreigingen ervan voor de samenleving. Van de Israëlische casus kan geleerd worden dat een bredere bewustwording van dit probleem van belang is om de dreigingen beter het hoofd te kunnen bieden. Ook is het principe van *flexibelere uitwisseling van kennis en ervaring* tussen verschillende organisaties, privaat en publiek en tussen verschillende sectoren, een leerpunt voor de Nederlandse situatie. Verder laat Israël duidelijk zien dat *cybersecurity* naast een dreiging ook een kans kan zijn voor economische ontwikkeling. De Israëlische casus laat echter ook zien dat veiligheid als belang (erg) dominant kan zijn en dat onder het mom van veiligheid en weerbaarheid rechtsstatelijke en democratische waarden onder druk kunnen komen te staan. De ontwikkeling van de *cybersecurity*industrie dient daarom hand in hand gaan met goed *toezicht* op de naleving van wet- en regelgeving op het terrein van fundamentele rechten (waaronder privacy).

Conclusies

De hoofdvraag die wij in dit onderzoek hanteren, luidt:

- *Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?*

Op grond van de landenstudies, en de vertaling naar Nederland, kunnen we de volgende conclusies trekken aangaande het gebalanceerd omgaan met de spanning tussen weerbaarheid en openheid.

Voor alles geldt dat de *dreigingsperceptie* van groot belang is voor de beslissingen rondom de inzet van veiligheidsmaatregelen. De dreigingsperceptie vertoont vaak een sterke *pad afhankelijkheid*, die niet alleen politiek is – politieke historie, politiek debat, politieke agenda's, et cetera – maar ook economisch en maatschappelijk. In Israël wordt de proactieve aanpak van *cyber*dreigingen op die manier alomvattend en 'unstoppable'. De Israëlische overheid is bijvoorbeeld sterk afhankelijk geraakt van innovaties en beslissingen in/van de private sector. Terwijl in Duitsland de aanpak van migratie meer principieel dan pragmatisch is, en vooral ook legitimiteit – in plaats van hoofdzakelijk effectiviteit – vooropstelt, zowel vanwege de maatschappelijke gedragen FDGO-principes, als het feit dat vluchtelingen als economisch kapitaal (werknemers) gezien worden.
In relatie tot pad-afhankelijke invloeden kunnen overheden ruimte creëren, mits ze de *dilemma's* van de weerbare open samenleving voor ogen houden. Het omgaan met die dilemma's zit, zo concluderen we op grond van de landenstudies en vertaling naar Nederland, in de volgende *mechanismen*.

Ten eerste, in beide cases gaat het niet enkel om het *pragmatisch* uitvoeren van bepaalde praktijken, maar ook om een *politiek debat* en vooral de *politieke framing* van de problematiek. In Israël en Duitsland wordt in politieke zin anders gekeken naar respectievelijk *cybersecurity* en het asiel- en migratievraagstuk dan in Nederland.
Ten tweede, in beide cases zetten landen een bepaalde koers in, maar is het tevens van belang dat ze *alert* en *adaptief* zijn en blijven. Naarmate een overheid meer op weerbaarheid gaat sturen, en een stevige koers inzet, kan dit ten koste gaan van de flexibiliteit om beleid en uitvoering snel aan te passen, en de koers te verleggen.

Ten derde, in beide cases en vooral in de Duitse casus zoeken overheden naar een balans tussen *stimuleren en regisseren*. In de Israëlische casus ligt de nadruk vanuit de overheid vooralsnog vooral op het stimuleren van innovaties en sturen op weerbaarheid waarbij beperkte aandacht is voor mogelijke gevolgen van deze ontwikkelingen voor privacy, mensenrechten, et cetera. Nederland lijkt juist de nadruk te leggen op de *regie* en *regulering*. De vraag in Nederland is dan ook meer, hoe kun je innovatie op het gebied van *cybersecurity* stimuleren met behoud van regie en controle? Bij regisseren hoort ook leren alsmede het borgen van de benodigde 'checks and balances'. In Duitsland zijn deze *basiswaarden* van de democratische rechtsstaat stevig verankerd in het denken en doen van de overheidsdiensten en diverse correctiemechanismen voorhanden als het gaat om de omgang van betrokken overheidsdiensten met asiel en migratie.

Aanbevelingen
Op grond van de bevindingen doen we een aantal aanbevelingen die voor overheden van belang zijn in het toewerken naar een WOS. We doen dat op basis van het *analysekader* zoals eerder gepresenteerd.

Dreigingsperceptie
1 *Wees realistisch en relativeer, accepteer dat niet alle dreigingen het hoofd kunnen worden geboden.* De overheid zal eerlijk moeten zijn over het feit dat niet alle potentiële dreigingen kunnen worden weggenomen of voorkomen.
2 *Houd de monitoring rond dreigingspercepties goed in het oog.* Om een strategie te ontwikkelen waarin overheidsinstanties adequaat kunnen anticiperen op het dynamische veld van dreigingspercepties is het noodzakelijk om goed zicht te houden op de uiteenlopende en veranderende percepties zoals dat reeds gebeurd in de Veiligheidsmonitor van het CBS en in de Risico en Crisisbarometer van de NCTV en dat mee te nemen in de beleidsvorming. Alleen op die manier kan de sociale constructie rondom een bepaalde dreiging begrepen worden, en kan de overheid zorgen voor een verhaal – *framing* –dat als legitiem wordt beschouwd.
3 *Wees voorbereid; ontwikkel een strategie om op wisselende dreigingspercepties te anticiperen*. Om legitiem te kunnen zijn moeten beleidsplannen en prakijken in overeenstemming zijn met de wat de burgers ervan verwachten. Daartoe is het niet alleen van belang dreigingen maar ook mogelijke dreigingspercepties in kaart te brengen en deze mee te nemen in het ontwikkelen van veiligheidspraktijken.

4 *Sta open voor verschillende percepties en principes*. Weeg af of het mogelijk is om in respectvolle dialoog over dreigingspercepties gesproken kan worden, waarbij zowel de zorgen en angsten worden geadresseerd als fundamentele principes van mensenrechten en openheid. Houd daarbij rekening met diverse maatschappelijke *onderstromen*.
5 *Maak jezelf en anderen bewust, werk aan veiligheidsscholing en educatie.* Via educatie kunnen burgers en professionals in (publieke en private) organisaties meer reflectievermogen en handelingsperspectieven ontwikkelen omtrent bepaalde mogelijke dreigingen, zodat zij ook daadwerkelijk hun eigen verantwoordelijkheid kunnen nemen. Ook is deze bewustwording van belang voor goed het laten landen van de gedachten achter de veiligheidspraktijken.

Veiligheidspraktijken en reflectie op waarden

1 *Wees legitiem, zoek naar steun en draagvlak.* Balanceren vraagt om legitimeren, bijvoorbeeld over de mate waarin we de rechten van het individu inperken in het geval van een crisis. In de ambtelijke voorbereiding zou dat expliciet meegewogen moeten worden.
2 *Maak expliciete afwegingen voorafgaand aan de inzet van maatregelen*. In het geval van een crisis wordt van de overheid verwacht dat zij het voorliggende probleem oplost. Voor de overheid is het dan belangrijk om te weten welke acties er moeten worden ondernomen en op welke manier die worden uitgelegd. Het is daartoe van belang om op voorhand een heldere boodschap te hebben, zodat betrokken actoren weten welk signaal er vanuit de overheid wordt gegeven in het geval van een bepaalde crisis. Om dit goed te kunnen doen, is het belangrijk om scenario's van potentiële crises uit te denken.
3 *Houd ook in evaluerende zin zicht op de legitimiteit van het beleid.* Het is van belang vooraf na te denken in hoeverre beleid gedragen zal worden, maar ook om de ontvangst van maatregelen te meten zodra een maatregel in praktijk is gebracht. Dit soort metingen van legitimiteit richten zich op het maatschappelijk vertrouwen (percepties van burgers) en houden rekening met mogelijk conflicterende waarden en belangen

Tot slot

Het beschermen van de waarden en belangen van de weerbare open samenleving (WOS) vraagt om een balanceer act van overheidsdiensten. Van de overheid wordt verwacht dat zij de samenleving beschermt tegen dreigingen. Dat moet krachtig, zichtbaar en op het eerste gezicht ferm dan wel 'met harde hand'. Maar naarmate de acties fermer en 'harder' zijn, wordt de onveiligheidsperceptie aangejaagd en de openheid en vrijheid van ons type samenleving op de proef gesteld, dan wel aangetast. Het vergt een *gevoelige* en *goed afgestemde governance* om hiermee om te kunnen gaan.

Dit start met het besef dat het niet om dilemma's maar om *paradoxen* gaat. Weerbaarheid en openheid staan niet naast of tegenover elkaar, maar moeten op elkaar betrokken worden. Het vraagt om een hoge mate van sensitiviteit voor mogelijke dreigingen en voor het zoeken naar overeenstemming tussen de betrokken actoren over die dreigingen. Dat vergt een goede antenne voor uiteenlopende meningen over dreigingen en over de wijzen waarop ze aangepakt zouden kunnen c.q. moeten worden.

Verder vraagt het om reflectie, zowel ex-ante als ex post, op het handelen van betrokken diensten in het omgaan met deze dreigingen, inclusief legitimiteit. In de weerbare open samenleving (WOS) wordt tegelijkertijd krachtig gehandeld, worden kritische vragen gesteld, worden afwegingen gemaakt en besproken en worden de onafhankelijke toetsing hiervan alsmede kritische reflecties hierop gegarandeerd.

Lijst van afkortingen

AfD:	Alternative für Deutschland
AIVD:	Algemene Inlichtingen- en Veiligheidsdienst
AVG:	Algemene verordening gegevensbescherming
AZC:	Asielzoekerscentrum
BAMF:	Bundesamt für Migration und Flüchtlinge
BfV:	Bundesamt für Verfassungsschutz
BKA:	Bundeskriminalamt
BVD:	Binnenlandse Veiligheidsidenst
CBS:	Centraal Bureau voor de Statistiek
CDA:	Christen-Democratisch Appèl
CDU:	Christlich Demokratische Union Deutschlands
CERT:	Computer Emergency Response Team
CERT-IL:	Computer Emergency Response Team - Israel
CEAS:	Common European Asylum System
COA:	Centraal Orgaan opvang Asielzoekers
CSBN:	Cybersecuritybeeld Nederland
CSU:	Christlich-Soziale Union
CU:	ChristenUnie
D66:	Democraten ’66
DNO:	Distribution Network Operator
DPolG:	Deutsche Polizei Gewerkschaft
DWR:	Digitale Werkomgeving Rijksdienst
EU:	Europese Unie
FDGO:	Freiheitliche Demokratische Grundordnung
FGGI:	Federal Government General Information
FvD:	Forum voor Democratie
GETZ:	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GTAZ:	Gemeinsames Terrormusabwehrzentrum
IBM:	International Business Machines Corporation
IDF:	Israel Defense Forces
INCB:	Israel National Cyber Bureau

INCD:	Israel National Cyber Directorate
IND:	Immigratie- en Naturalisatiedienst
IS:	Islamitische Staat
IT:	Informatietechnologie
LFV:	Landesfeuerwehrverband
LKA:	Landeskriminalamt
MIVD:	Militaire Inlichtingen- en Veiligheidsdienst
MKB:	Midden- en kleinbedrijf
NCSA:	Nederlandse Cybersecurity Agenda
NCSC:	Nationaal Cyber Security Centrum
NCTV:	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NISA:	Netherlands Intelligence Studies Association
NVP:	Nationaal Veiligheidsprofiel
PKK:	Koerdische Arbeiderspartij
PvdA:	Partij van de Arbeid
PVV:	Partij Voor de Vrijheid
RIVM:	Rijksinstituut voor Volksgezondheid en Milieu
SP:	Socialistische Partij
SPD:	Sozialdemokratische Partei Deutschlands
UNHCR:	United Nations High Commissioner for Refugees
USBO:	Utrechtse School voor Bestuurs- en Organisatiewetenschap
VN:	Verenigde Naties
VUCA:	Volatile, Uncertain, Complex, Unambiguous
VVD:	Volkspartij voor Vrijheid en Democratie
Wiv:	Wet op de inlichtingen- en veiligheidsdiensten
WODC:	Wetenschappelijk Onderzoek- en Documentatiecentrum
WOS:	Weerbare open samenleving
WRR:	Wetenschappelijke Raad voor het Regeringsbeleid

1. Introductie

1.1 INLEIDING

Veiligheidsdenken heeft in westerse samenlevingen stevig postgevat. Over westerse samenlevingen wordt zelfs gesproken in termen van 'security societies' of 'societies of control' (Garland, 2001). Dreigingen, zo is het breed gedragen beeld, zijn steeds meer gaan voldoen aan de kenmerken van een 'VUCA' wereld. De dreigingen veranderen snel en zijn onvoorspelbaar van aard (*Volatile*), ze zijn omgeven met onzekerheid over wat er staat te gebeuren (*Uncertain*), ze zijn ingewikkeld door de veelheid aan krachten die erop van invloed zijn (*Complex*) en oorzaak en gevolg zijn onduidelijk en moeilijk verklaarbaar (*Ambiguous*).

Diverse dreigingsanalyses (Clingendael, 2017; Nationaal Cyber Security Centrum, 2017; NCTV, 2016, RIVM, 2016) laten zien dat de dreigingen/verstoringen zich in snel veranderende en steeds complexere vorm aandienen. Denk aan grensoverschrijdende *cyber*criminaliteit, geopolitieke verschuivingen, extremistische en terroristische aanslagen en klimaatverandering. Daar komt bij dat de binnenlandse en buitenlandse veiligheid in toenemende mate met elkaar verweven zijn geraakt. Dit betekent dat dreigingen op een internationaal niveau direct gevolgen kunnen hebben voor de Nederlandse samenleving. Minister Bijleveld (Ministerie van Defensie, 2018) zegt hierover in een brief aan de kamer over de toekomst van Defensie. "Nederland en Europa worden geconfronteerd met een complex, divers en onzeker dreigingsbeeld. Onze waarden en belangen staan hierdoor op het spel."

De overheid stelt zichzelf de opgave om de (vaak nog niet bekende) risico's te beteugelen, *'taming of the future'* (De Graaf, 2013). Zij doen dit door de weerbaarheid van de samenleving tegen deze dreigingen te verhogen en er op een gepaste en gecoördineerde wijze mee om te gaan, met de continue inachtneming van de onderliggende waarden van onze democratische rechtsstaat (zie hoofdstuk 2 voor een verdere toelichting op deze onderliggende waarden). De overheid zoekt naar wegen om tijdig en afgestemd te kunnen reageren op nieuwe dreigingen. In de Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 wordt dit als volgt geformuleerd:

"*De dreiging die uitgaat van terroristische aanslagen, cyberaanvallen, ongewenste buitenlandse inmenging en ondermijning, militaire druk en aanvallen op vitale economische processen is urgent en vraagt om effectief veiligheidsbeleid."* (Ministerie van Buitenlandse Zaken, 2018, blz. 6).

De overheid werkt op vele fronten aan de versterking van de binnenlandse en buitenlandse veiligheid. Dat dit een uiterst complexe opgave is, behoeft weinig toelichting. Want hoe ontwerpen we maatregelen voor nog onbekende dreigingen? En hoe voorkomen we dat de diversiteit aan dreigingen leidt tot een oneindig breed scala aan (beleids)maatregelen, preventieve interventies en curatieve acties? Zo wordt er op veel verschillende beleidsterreinen beleid ontwikkeld dat tot doel heeft de aanpak van dreigingen te versterken, waaronder de versterking en modernisering van de krijgsmacht (Ministerie van Defensie, 2018), het beleid op het gebied van buitenlandse handel- en ontwikkelingssamenwerking (Ministerie van BuZa, 2018), de geïntegreerde buitenland- en veiligheidsstrategie, inclusief internationale politiestrategie en migratieagenda (Ministerie van BuZa, 2018), de Nederlandse cybersecurity agenda (Ministerie van V&J, 2017), de digitaliseringsagenda (Ministerie van EZK, 2018), de nationale contraterrorismestrategie (NCTV, 2016) en het nationaal handboek crisisbesluitvorming (NCTV, 2016). Maar hoe stemmen we vervolgens deze maatregelen op elkaar af en hoe passen we dit brede scala aan (beleids)maatregelen snel genoeg aan om het tempo van de snel veranderende (digitale) dreigingen bij te kunnen benen?

Ondanks alle inspanningen zal de overheid nooit geheel voorbereid kunnen zijn op alle verschillende dreigingen die zich kunnen voordoen in deze VUCA-wereld. Om de dreigingen en bijbehorende respons meer op elkaar te kunnen afstemmen, is het nodig om zowel de *sensitiviteit* voor potentiële dreigingen als de *flexibiliteit* van (beleids)maatregelen en -acties te vergroten. Het is niet verwonderlijk dat vooral stevig ingezet wordt op flexibiliteit,[2] zoals de flexibilisering van de nationale crisisorganisatie[3] en een nauwe afstemming tussen de verschillende spelers binnen de overheid en tussen publieke en private partijen (NCTV, 2016).

Het kabinet heeft in september 2016 aan de Kamer toegezegd dat een strategische visie voor de komende jaren zal worden opgesteld waarin wordt vastgelegd op welke manier de nationale veiligheid zo goed mogelijk kan worden versterkt (Kamerstukken II, 2015-2016). In zijn reactie op het WRR-rapport 'Veiligheid in een wereld van verbindingen' heeft het kabinet in maart 2018 aangekondigd dat door de ministeries van BZ, Defensie en JenV gezamenlijk zal worden gewerkt aan een geïntegreerde dreigingsaanpak op basis van een geïntegreerde dreigingsanalyse, de Defensienota en de Geïntegreerde Buitenland- en Veiligheidsstrategie (Kamerstukken II, 2017-2018).

---

2 Voortgangsbrief nationale veiligheid 2015 https://www.nctv.nl/binaries/voortgangsbrief-nationale-veiligheid-12-mei-2015_tcm31-29624.pdf

3 Voortgangsbrief nationale veiligheid 2016 file:///C:/Users/schif103/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/TK+Voortgangsbrief+Nationale+Veiligheid.pdf

1.2 DOEL EN VRAAGSTELLING

1.2.1 Doel

Doel van dit onderzoek is het aanleveren van bouwstenen voor de discussie over de omgang met complexe veiligheidsuitdagingen waar de Nederlandse overheid zich voor gesteld ziet, in het bredere kader van de veelheid aan (snel) veranderende dreigingen. Meer specifiek zoeken we naar voorstellen en praktijkvoorbeelden uit binnen- en buitenland die laten zien welke realistische en haalbare capaciteiten worden ingezet en welke (technische) maatregelen worden genomen, hoe dat gebeurt en door wie op mogelijk toekomstige dreigingen wordt geanticipeerd en gereageerd. Bij de reacties letten we er op welke stappen genomen worden, welke juridische/ organisatorische/economische capaciteiten daarop ingezet worden en hoe deze reacties zich verhouden tot de belangen die verdedigd dienen te worden. Daarvoor hanteren wij het concept van de weerbare open samenleving (WOS). Dit concept, dat verder uitgewerkt wordt in hoofdstuk 2 van dit rapport gaat uit van een *balans* die gevonden kan worden tussen enerzijds het weerbaar maken van een samenleving en anderzijds het beschermen van de open samenleving met inachtneming van democratische en rechtsstatelijke waarden.

Dit onderzoek richt zich daarbij aan de hand van een tweetal casus op de wijze waarop dreigingen binnen een samenleving geduid worden (*Wat wordt er bedreigd en wat dient er verdedigd te worden?*), de wijze waarop de respons erop ingezet en georganiseerd wordt (*Hoe wordt de dreiging aangepakt? Welke praktijken worden daarin gehanteerd en hoe wordt dat georganiseerd?*) en welke mogelijke consequenties dat heeft voor de weerbare open samenleving? (*Welke belangen worden met de ingezette praktijken verdedigd en welke komen mogelijk onder druk te staan?*).

De uiteindelijke waarde van dit onderzoek ligt in de handreikingen en inzichten die we bieden aan het ministerie van J&V, de NCVT en partners zodat zij de open samenleving en haar democratische en rechtsstatelijke waarden (nog beter) kunnen beschermen. Het is daarvoor belangrijk om verschillende internationale cases goed te begrijpen, maar ook om kennis te hebben van het Nederlandse veld, om een passende en bruikbare vertaling van inzichten te maken.

1.2.2 Vraagstelling

De hoofdvraag die wij in dit onderzoek hanteren luidt:

- *Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?*

Deze hoofdvraag is nog erg ruim en is om redenen van onderzoekbaarheid teruggebracht naar het uitwerken van twee specifieke verstoringen/dreigingen in andere landen die naar verwachting van belang zijn voor de Nederlandse context. In dit onderzoek wordt daartoe een tweetal *experienced cases* beschreven van westerse democratieën en hun omgang met een complexe, grensoverschrijdende dreiging/verstoring. Doel van de casuïstiek is het ophalen van mogelijke lessen ten behoeve van de Nederlandse aanpak van snel veranderende dreigingen in het algemeen en de betreffende dreiging in het bijzonder.

In de zoektocht naar geschikte casuïstiek is in overleg met de begeleidingscommissie (zie paragraaf 1.3) van dit onderzoek gekozen voor de volgende twee casus (voor een uitgebreidere toelichting op deze landenselectie zie hoofdstuk 3):

- *Duitsland*: Omgaan met migrantenstromen
- *Israël*: Afwending van *cyber*aanvallen

Aan de hand van de landencasuïstiek wordt gezocht naar antwoorden op de volgende deelvragen:

1 Welke dreiging zien deskundigen in de betreffende landen rondom de gekozen thematiek voor de weerbare open samenleving? Welke waarden en belangen zijn daarbij beschermwaardig?
2 Welke praktijken worden gehanteerd om deze dreigingen het hoofd te bieden:
   a Welke mogelijkheden zien deskundigen in de betreffende landen om met technologische middelen of anderszins, disruptieve maatschappelijke ontwikkelingen in een vroegtijdig stadium te voorzien?
   b Wat is de uitvoerbaarheid van deze maatregelen?
   c Welke gevolgen hebben de snelle veranderingen van de dreigingen voor de (interne) organisatie van zowel private als publieke betrokken partijen en wat betekent dit voor de benodigde capaciteit[4]?
   d In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?
3 Welke mogelijke gevolgen hebben de ingezette praktijken voor de weerbare open samenleving?

Vervolgens worden deze bevindingen getoetst aan en geplaatst in de Nederlandse context. Daarmee wordt toegewerkt naar het beantwoorden van de onderstaande deelvragen:

---

[4] De term “capaciteit” wordt breed opgevat. Het kan gaan over in te zetten mankracht, materieel, maar ook over voldoende (beleids)maatregelen/instrumenten om een bepaalde dreiging aan te pakken.

Weerbaarheid van de Nederlandse samenleving en organisaties

1 Wat kan Nederland leren van de betreffende landenpraktijken voor de inzet van maatregelen voor de weerbare open samenleving?
2 Wat kunnen de snel veranderende problematieken/dreigingen rondom onder meer asiel- en migratieproblematiek en *cybersecurity* betekenen voor (afstemming tussen) werkprocessen van de Nederlandse (overheids)organisaties die verantwoordelijk zijn voor het Nederlandse veiligheidsbeleid, onder meer als het gaat om agendering en besluitvorming, en welke capaciteiten zijn zowel kwantitatief als kwalitatief (competenties) nodig om de weerbaarheid van de Nederlandse overheidsorganisaties te versterken?

1.3 ORGANISATIE INVENTARISEREND ONDERZOEK

Het WODC heeft het departement Bestuurs- en Organisatiewetenschap (USBO Advies) van de Universiteit Utrecht gevraagd dit inventariserend onderzoek uit te voeren. Met het oog op de bovenstaande doel- en vraagstelling heeft USBO-expertise binnen de Universiteit Utrecht betrokken, op de terreinen van weerbaarheid, *'sense and respond'*, rechtsstatelijke en democratische waarden en veiligheidsbeleid. Onderhavig rapport betreft dan ook een *multidisciplinair* onderzoek, waarbij de problematiek vanuit de disciplines bestuurs- en organisatiewetenschap, rechtsgeleerdheid en geschiedenis is bestudeerd. Daarnaast is een expertgroep van hoogleraren betrokken om te reflecteren op de gegenereerde onderzoeksresultaten, en om het kernteam van onderzoekers op verschillende momenten te voorzien van belangrijke kennis en inzichten op het gebied van onder meer de impact op de samenleving van diverse dreigingen waaronder terrorisme (prof. dr. Beatrice de Graaf en prof. dr. Kees van den Bos), de rol van staatsrechtelijke waarden (prof. dr. Henk Kummeling), de organisatie van overheidsoptreden (prof. dr. Mirko Noordegraaf) en de rol van leiderschap in situaties van dreiging (prof. dr. Paul 't Hart). Voor een meer gedetailleerde uitwerking van het projectteam en de betrokken experts, verwijzen wij u naar de bijlage IV.

Door het WODC is verder een begeleidingscommissie ingesteld die kritisch meedenkt in alle fasen van het onderzoek en het projectteam van feedback voorziet op (tussen)rapportages. De begeleidingscommissie bestond uit voorzitter prof. dr. Arjen Boin (Instituut Politieke Wetenschap, Universiteit Leiden), dr. Irna van der Molen (Centre for Risk management, Safety and Security, Universiteit Twente), mr. Cees Pisuisse (Commissielid 'Vitale Infrastructuur'), prof. dr. Peter Bos (Veiligheidsregio Utrecht), drs. Geert Wismans (NCTV), en dr. Gerrit Haverkamp (WODC).

1.4 LEESWIJZER

In dit rapport komen achtereenvolgens de volgende hoofstukken aan de orde. Na deze introductie beschrijven we in hoofdstuk 2 het analysekader waarin de in dit onderzoek gehanteerde concepten en hun onderlinge samenhang toegelicht wordt.

In hoofdstuk 3 wordt een toelichting gegeven op de gehanteerde onderzoeksmethodiek en de landenselectie. In de hoofdstuk 4 wordt de Duitse asiel- en migratiecasus beschreven, gevolgd door de vertaalslag van deze Duitse casus naar de Nederlandse context (hoofdstuk 5). In hoofdstuk 6 gaan we in op de Israëlische *cybersecurity*casus, gevolgd door een vertaalslag van deze casus naar de Nederlandse situatie in hoofdstuk 7. Tot slot worden in hoofdstuk 8 conclusies getrokken en concrete aanbevelingen gedaan op basis van de in de voorgaande hoofdstukken beschreven bevindingen.

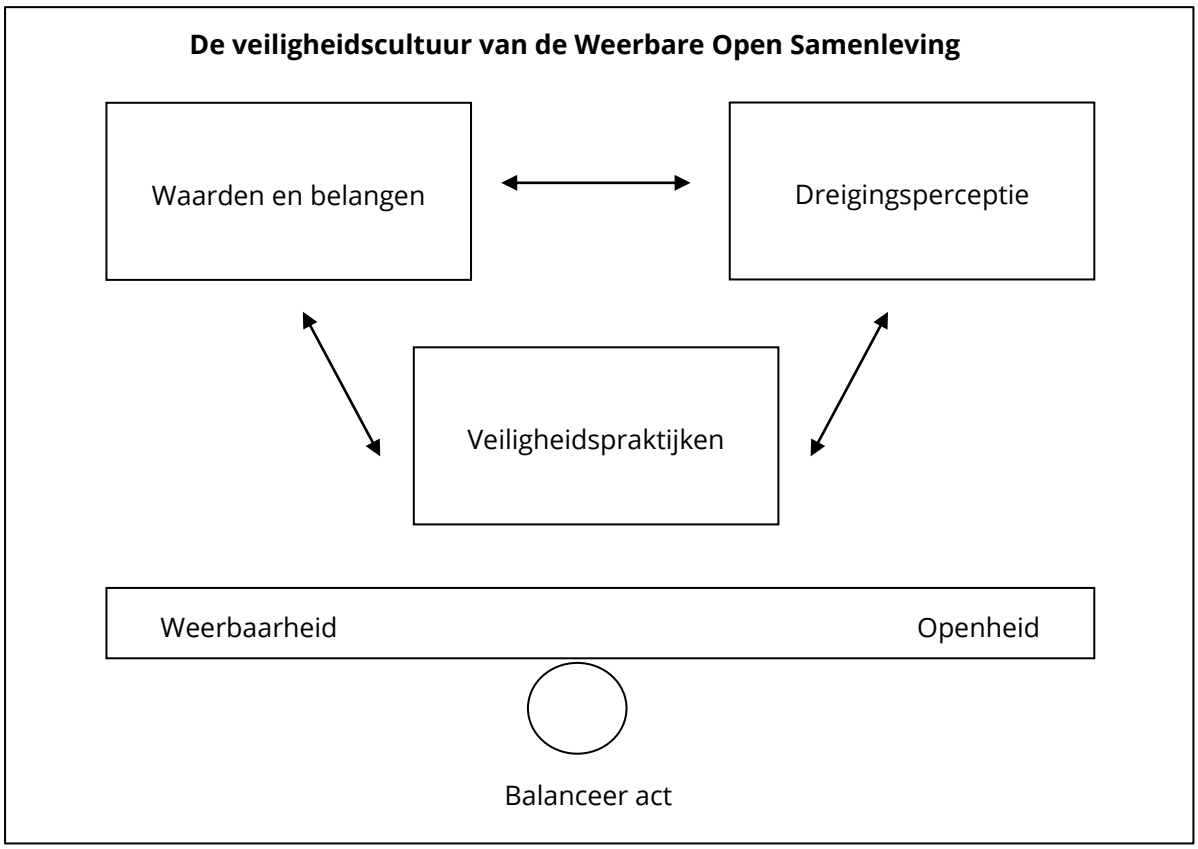
2. Analysekader

2.1 INTRODUCTIE

In dit hoofdstuk presenteren we het analysekader, zoals gehanteerd in de landencasuïstiek, en werken we de kernconcepten van dit kader nader uit. In het analysekader staan de begrippen die samen de *veiligheidscultuur* van een land vormen centraal. Onder 'veiligheidscultuur' verstaan we hoe in een land in brede zin met veiligheid wordt omgegaan, inclusief attitudes, percepties en meningen ten aanzien van de gewenste mate van veiligheid, beschermwaardige belangen, ervaren dreigingen en gewenste en geaccepteerde praktijken om de dreiging te beteugelen (De Graaf, 2014, p.9). De veiligheidscultuur zal beïnvloeden hoe overheden en andere actoren op dreiging reageren, waarom, en wat de gevolgen daarvan zijn. Qua gevolgen kijken we vooral naar de wijze waarop zowel *weerbaarheid* als *openheid* worden gerealiseerd, waarbij deze maatschappelijke waarden elkaar kunnen bijten, of juist versterken. Wat in specifieke landen aangaande concrete issues plaatsvindt in termen van de veiligheidscultuur en de afwegingen die daarbij worden gemaakt, is vervolgens inzet van empirisch onderzoek.

In dit hoofdstuk worden de centrale elementen die samen de veiligheidscultuur van een samenleving vormen uiteengezet. Figuur 1 biedt een overzicht van de betreffende centrale begrippen die nodig zijn voor de uitwerking van de onderzoeksvragen zoals beschreven in hoofdstuk 1. We starten met een nadere uitwerking van de concepten veiligheidscultuur (par. 2.2) en de 'weerbare open samenleving' (WOS) (par. 2.3). Bij de beschrijving van de weerbare open samenleving wordt ook uitgewerkt welk type belangen beschermwaardig worden geacht in weerbare open samenlevingen. Vervolgens wordt toegelicht welke ontwikkelingen in onze westerse samenlevingen gepercipieerd worden als een dreiging voor deze beschermwaardige belangen (par. 2.4) en met welk type veiligheidspraktijken en -maatregelen deze dreigingen worden aangepakt (par.2.5). Tot slot wordt aandacht besteed aan de 'balanceer act' die nodig is in een WOS om het evenwicht tussen de belangen behorende bij weerbaarheid en openheid te behouden.

Figuur 1. Analysekader



2.2 VEILIGHEIDSCULTUUR

De veiligheidscultuur geeft – simpel gezegd – aan hoe er in een samenleving tegen veiligheid wordt aangekeken en met veiligheid wordt omgegaan. Het gaat daarbij uiteindelijk om het beleid en de procedures die in gang worden gezet om de veiligheid te waarborgen, maar bovenal ook om de achterliggende attitudes, percepties en meningen (veiligheidsdenken) over beschermwaardige belangen, dreigingen en de maatregelen die genomen moeten worden om deze dreigingen het hoofd te bieden.

"[...] studies over veiligheidsdenken hebben tot doel om te begrijpen (a) wie bevoegd is om te beveiligen; (b) tegen welke dreigingen; (c) wie of wat er wordt beveiligd; (d) waarom diegene of datgene wordt beveiligd; (e) met welke resultaat; en (f) en onder welke omstandigheden (zodat kan worden uitgelegd wanneer deze vorm van veiligheid succesvol is)" (Buzan et al., 1998, p.32).

Voortbouwend op bovenstaande aspecten werd het begrip veiligheidscultuur geïntroduceerd waarbij voor een specifieke situatie de gepercipieerde belangen, dreigingen en veiligheidsmaatregelen worden beschreven (De Graaf, 2017).

2.3 VEILIGHEIDSCULTUUR IN WEERBARE OPEN SAMENLEVINGEN

In dit onderzoek kijken we naar de veiligheidscultuur van samenlevingen die *tegelijkertijd* weerbaar en open willen zijn. Dat vraagt om een continue 'balanceer act' tussen twee grootheden die elkaar kunnen versterken maar elkaar ook kunnen ondermijnen.

De Graaf (2014, p.7) formuleerde drie vragen om de veiligheidscultuur voor een specifieke situatie te beschrijven:

1 Welke waarden en belangen vinden wij beschermwaardig?
2 Wie en/of wat zien wij als potentiële dreigingen?
3 In welke veiligheidspraktijken vertaalt zich dat?

Deze conceptualisering van de 'veiligheidscultuur' dient als theoretische drieslag in de verschillende hoofdstukken. In dit onderzoek richten we ons op deze drie deelvragen en het samenspel daartussen binnen de context van een weerbare open samenleving. We inventariseren wat dit samenspel ons leert over de wijze waarop in een specifieke context wordt omgegaan met een specifieke grensoverschrijdende dreiging en wat Nederland van die werkwijze kan leren. Dit wordt telkens gekoppeld aan de afwegingen die gemaakt worden tussen openheid en weerbaarheid in het omgaan met de dreigingen en dus het vormgeven van de praktijken. Om beter te begrijpen waar we op doelen met een weerbare open samenleving biedt onderstaand kader een nadere definitie hiervan.

Weerbare Open Samenleving (WOS)
De term 'weerbare open samenleving' (WOS) is een samenvoeging van de termen weerbare samenleving en open samenleving. In dit kader is uitgewerkt wat in we in dit onderzoek verstaan onder de 'open samenleving' en de 'weerbare samenleving' en onder de combinatie van beiden.

Open samenleving
Sinds de jaren '30 van de vorige eeuw wordt in wetenschappelijke literatuur geschreven over de open samenleving (bijv. Bergson, 1932; Loewenstein, 1937a; Loewenstein, 1937b; Popper, 1945). De open samenleving wordt veelal gelijkgesteld aan de democratische rechtsstaat, die het legaliteitsbeginsel, de machtenscheiding (trias politica), de grondrechtenbescherming, de onafhankelijke rechterlijke controle en de democratie, als haar vijf grondbeginselen koestert (Burkens et al., 2017) (zie voor een nadere uitwerking van de beschermwaardige waarden en belangen van de open samenleving par. 2.4).

Het huidige politieke debat met betrekking tot openheid is redelijk eensgezind. Hier wordt het concept openheid veelal wordt gebruikt in relatie tot het tolereren van uiteenlopende denkbeelden en het bestrijden van discriminatie (VVD, CDA, D66, GroenLinks, PvdA en CU). Deze invulling richt zich dus vooral op grondrechtenbescherming. Het kabinet refereert in een reactie op het WRR rapport uit 2017 vanuit nog een andere invalshoek aan de open samenleving, getuige het volgende citaat: "De dreigingen die met deze ontwikkelingen gepaard gaan, raken Nederland als open samenleving met een internationale oriëntatie rechtstreeks. Nederland dankt zijn welvaart immers in belangrijke mate aan het grensoverschrijdend verkeer van ideeën, personen, goederen en data".

De open samenleving wordt dus op verschillende wijzen geïnterpreteerd. Wij grijpen in dit onderzoek terug de meer oorspronkelijk betekenis van de open samenleving zoals beschreven door Karl Popper in zijn klassieke werk: *The Open Society and its Enemies* (1945). Daarin verwijst de open samenleving voor een samenleving waarin wetten, gewoontes en instituties openstaan voor correctie. Leden van een open samenleving kunnen openlijk haar instituties en machtsstructuren bekritiseren, zonder bang te hoeven zijn voor represailles.

Weerbare samenleving
Over de invulling die de politiek geeft aan weerbaarheid bestaat verdeeldheid. Zo benadrukken sommige van de meest recente verkiezingsprogramma's (2017-2021) het belang van het vergroten van de weerbaarheid van individuen (D66, CDA, SP en CU) dan wel van economische, juridische en digitale systemen (VVD, CDA en D66), terwijl andere politieke partijen de term weerbaarheid niet als zodanig gebruiken in hun programma's. Voor de definiëring van de termen 'weerbaarheid' en 'weerbare samenleving' maken wij gebruik van de omschrijvingen zoals gehanteerd in de weerbaarheidsmonitor opgesteld door TNO in opdracht van het WODC (TNO, 2014). Zij definiëren weerbaarheid als het vermogen van een individu, gemeenschap of systeem tot weerstand, veerkracht en aanpassing indien een verstoring van de als normaal ervaren toestand optreedt.'

"Bij weerstand gaat het om het vermogen van het systeem om door te kunnen gaan met zijn functie indien een verstoring optreedt, zonder dat het systeem daardoor een significante verandering ondervindt. Als functies wel worden aangetast dan zorgt veerkracht ervoor dat het functioneren wordt hersteld. Adaptiviteit is het vermogen van een systeem om op veranderingen in hun omgeving te reageren, zich aan te passen en te leren van ervaringen." "Een weerbare maatschappij is een maatschappij waarin individuen, groepen en gemeenschappen in staat zijn om te gaan met dreigingen en verstoringen als gevolg van sociale, economische en fysieke veranderingen".

Het gaat daarbij om de weerbaarheid van de samenleving als geheel tegen verstoringen van binnen of buiten. De weerbaarheid van instituties vormt hier een onderdeel van.

Weerbare Open Samenleving (WOS)
Democratische rechtsstaten willen open staan voor verschillende overtuigingen in de samenleving en tegelijkertijd weerbaar zijn tegen (potentiële) verstoringen en antidemocratische dreigingen. Zij investeren in weerbaarheid teneinde de waarden en belangen een de democratische rechtsstaat te kunnen waarborgen. Weerbaarheid staat daarmee in dienst van de open samenleving. In het licht van Bourbeau's (2013) publicatie over weerbaarheid behoort deze doelstelling tot de categorie 'resilience as maintenance': de rechtsstatelijke en democratische status quo moet behouden blijven. In de praktijk blijkt dit echter vaak een lastige balanceeract te zijn waarbij het risico bestaat dat een te stevige inzet op weerbaarheid ten koste kan gaan van de openheid of waarbij een te sterke focus op openheid een wissel kan trekken op de weerbaarheid. In beide gevallen is de balans verstoord, hetgeen zal leiden tot ongewenste effecten voor de beschermwaardige waarden en belangen van de WOS. Het kabinet refereert aan deze balanceer act als het behouden van het "evenwicht tussen veiligheid en vrijheid" (NCTV, 2016). Hoe aan deze balanceer act in de praktijk vormgegeven wordt, wordt geïllustreerd aan de hand van de landencasuïstiek.

2.4 BESCHERMWAARDIGE WAARDEN EN BELANGEN

In de voortgangsbrief Nationale veiligheid van het kabinet staat dat in het omgaan met risico's en dreigingen het behoud van de democratische rechtstaat centraal staat (NCTV, 2016). In een democratische rechtsstaat gelden vijf beginselen (Burkens et al., 2017) die tevens te bezien zijn als beschermwaardige (kern)waarden van weerbare open samenlevingen:

1 *Legaliteitsbeginsel*: het overheidsoptreden waardoor burgers gebonden worden – in hun vrijheden beperkt worden – berust op een wettelijke grondslag;
2 *Machtenscheiding*: de overheidsmacht is verdeeld over drie onderscheiden functies, te weten de wetgevende, uitvoerende en rechtsprekende macht;
3 *Grondrechtenbescherming*: bepaalde fundamentele rechten en vrijheden worden gewaarborgd, en de overheid spant zich in om de voorwaarden voor grondwettelijke vrijheidsuitoefening voor burgers te verwezenlijken;
4 *Onafhankelijke rechterlijke toetsing*: al het overheidshandelen is onderworpen aan rechterlijke rechtmatigheidscontrole; burgers die door overheidshandelen in hun belang worden getroffen, hebben toegang tot een onafhankelijke rechterlijke macht;
5 *Democratie*: de uitvoerende macht heeft een verantwoordingsplicht ten opzichte van de volksvertegenwoordiging die is gekozen in vrije en periodieke verkiezingen.

Verder staan in de Strategie Nationale Veiligheid (NCTV, 2007) de volgende vijf nationale veiligheidsbelangen omschreven.

Territoriale veiligheid	Het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin.
Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving.
Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie.
Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland.
Sociale en politieke stabiliteit	Het ongestoorde voorbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleving binnen de verworvenheden van de Nederlandse democratische rechtsstaat en daarin gedeelde waarden.

Daarnaast staat in de Geïntegreerde Buitenland- en Veiligheidsstrategie van het Ministerie van Buitenlandse Zaken (2018, p.11) het volgende over het belang voor Nederland van een veilige: *"Nederland kent een rijke traditie op het gebied van internationale samenwerking. Als handelsland is Nederland sterk internationaal georiënteerd. Dit is een van de redenen waarom ons land belang heeft bij een veilige wereld. De wereldwijde inzet voor een veilig Koninkrijk is gestoeld op het Statuut van het Koninkrijk, de Nederlandse grondwet, het Europese Verdrag van de Rechten van de Mens, het internationaal recht en de democratische kernwaarden waarop onze rechtstaat is gebouwd. Nederland is ervan overtuigd dat duurzame vrede en veiligheid zijn gebaat bij een mensgericht en inclusief beleid, zoals ook de WRR bepleit: bescherming van burgers – vrouwen en kinderen in het bijzonder – in lijn met de nationale agenda van VNVR-resolutie 1325 over vrouwen, vrede en veiligheid, maakt onlosmakelijk onderdeel uit van ons geïntegreerd buitenland- en veiligheidsbeleid. Dit vormt het normatieve kader waarbinnen het kabinet opereert en bepaalt hoe Nederland beleidsinstrumenten inzet en welke partnerschappen het vormt."*

Tot slot is het van belang te vermelden dat de beschermwaardige waarden en belangen lang niet altijd in elkaars verlengende liggen, en dat er met regelmaat sprake is van conflicterende situaties waarbij het inzetten op het ene belang, het andere belang (deels) kan verdringen. Bij de afweging tussen deze verschillende waarden en belangen kan er logischerwijze sprake zijn van drie verschillende scenario's:

1 Een keuze tussen *CONFLICTERENDE* waarden en belangen. Het gaat in deze gevallen om tegenover elkaar staande waarden en belangen waarbij het tegemoetkomen aan de ene waarde ten koste kan gaan van de andere waarde. Dit scenario wordt gekenmerkt door *OF-OF* situaties.
2 Een *VERVLECHTING* van waarden en belangen waarbij sprake is van het kunnen combineren van waarden en belangen. Hierbij is sprake van *EN-EN* situaties.
3 Een *SAMENGAAN* van diverse waarden en belangen. De waarden en belangen versterken elkaar waardoor nieuwe realiteiten en kansen worden gecreëerd. Er is sprake van *WIN-WIN* situaties.

Vooral de eerste categorie betreft de lastige afwegingen waarbij meer weerbaarheid kan leiden tot minder openheid of meer openheid leidt tot minder weerbaarheid (Zie paragraaf 2.7 voor een verder uitwerking van de balanceer act). Bij het beschermen van de onderliggende waarden en belangen dient dus telkens geëxpliciteerd te worden welke waarden en belangen in het geding zijn, welke eerst en vooral beschermd dienen te worden, volgens wie en waarom.

2.5 DREIGINGSPERCEPTIE

Diverse dreigingsanalyses (Clingendael, 2017; Nationaal Cyber Security Centrum, 2017; NCTV, 2016, RIVM, 2016) beschrijven ontwikkelingenrisico's die gepercipieerd worden als dreigingen/verstoringen voor onze samenleving. De analyses zijn vrij eensluidend in de constatering dat de dreigingen zich in snel veranderende en steeds complexere vorm aandienen.

Denk aan grensoverschrijdende *cyber*criminaliteit, geopolitieke verschuivingen, extremistische en terroristische aanslagen en klimaatverandering. Boin (2017) beschrijft deze veranderde aard van (potentiële) dreigingen in vijf kenmerken:

1 De dreigingen omvatten meerdere sectoren, landen en crises;
2 De dreigingen kunnen ontstaan in (plotselinge) zeer snelle escalaties in periodes van trage evolutie doordat internationale verwevenheid is toegenomen, problemen complexer zijn geworden, en het aantal actoren sterk is toegenomen;
3 De oorzaken, gevolgen en momenten van escalaties die leiden tot de dreigingen zijn moeilijk te begrijpen;
4 Uiteenlopende actoren en bestuurslagen zijn in de dreigingen betrokken, soms met botsende verantwoordelijkheden;
5 De dreigingen kennen geen pasklare oplossingen, en de gekozen oplossingen leiden zelf weer tot nieuwe problemen, soms op andere plekken.

De complexiteit en de veranderde aard van deze dreigingen maakt dat mogelijke gevaren voor de open samenleving minder eenvoudig te vatten én op te lossen zijn. Dit komt vooral doordat dreigingen grenzeloos zijn geworden (Boin, 2017): voor de (potentiële) dreigers bestaan de grenzen van de open samenleving, en daarmee van de democratische rechtsstaat, niet. Daar komt bij dat als gevolg van de veranderde aard van (potentiële) dreigingen geldt dat mogelijk toegebrachte schade zich niet beperkt tot een afgebakende tijd of ruimte. Integendeel, (potentiële) dreigingen zijn in toenemende mate grensoverschrijdend, generatie-overschrijdend, onvoorspelbaar, en kunnen zich voordoen in alle maatschappelijke domeinen van de samenleving (Geldof, 2015).

Zo constateert de WRR dat de veiligheidssituatie voor Nederland de afgelopen jaren is verslechterd en veranderd (WRR, 2017). Verschillende ontwikkelingen elders hebben volgens de WRR 'direct of indirect' invloed op de veiligheidssituatie in Nederland zoals het neerschieten van vlucht MH17 boven Oekraïens grondgebied, de komst van vluchtelingen als gevolg van burgeroorlogen in het Midden-Oosten en Afrika, de strijd met terreurbeweging IS in Syrië en Irak, de terugkomst van Syriëgangers, terroristische dreigingen in Europa, bedreigingen via *cyber* (hacken, desinformatie) en de spanningen na de mislukte putsch in Turkije van 15 juli 2016 en rond het Turkse constitutionele referendum. Deze ontwikkelingen brengen grensoverschrijdende dreigingen met zich mee waarbij binnenlandse en buitenlandse veiligheid steeds meer in elkaar grijpen.

In een reactie op het WRR-rapport geeft het kabinet aan dat de dreigingen die te maken hebben met de instabiliteit in de landen rondom Europa, Nederland rechtstreeks raken als open samenleving met een internationale oriëntatie. De dreigingen worden als volgt omschreven (Kamerbrief over adviesrapport WRR, 2018)*: "De veiligheid van de Nederlandse bevolking is mede afhankelijk geworden van de leefomstandigheden van mensen in het Midden- Oosten en in Noordelijk*

Afrika. Tegelijkertijd is Rusland in Europa een onvoorspelbare factor geworden door het destabiliserende optreden van dat land in Oekraïne en zijn de dreigingen in het digitale domein gegroeid".
De brede schakering aan potentiële dreigingen voor Nederland met hun mogelijke impact staan beschreven in het Nationaal Veiligheidsprofiel (RIVM, 2016). In dit onderzoek is ervoor gekozen de focus te leggen op een aantal specifieke potentiële verstoringen/dreigingen voor de waarden en belangen van onze open samenleving. Structurele aantasting van de democratische rechtsstaat en de waarden van onze open samenleving komen in het Nationaal Veiligheidsprofiel voor in de scenario's bij de thema's 'Geopolitieke dreigingen', 'Ondermijning, extremisme en terrorisme', 'Financieel-economische bedreigingen' en de risicocategorie '*Cyber*spionage'.
Voor een beschrijving van de dreigingen zoals gesignaleerd in respectievelijk Duitsland en Nederland rondom de asiel en migratieproblematiek zie hoofdstuk 4 en 6 en voor de dreigingen zoals gesignaleerd ten aanzien van *cybersecurity* in respectievelijk Israël en Nederland zie hoofdstuk 5 en 6.

Veel dreigingen hebben te maken met een pluriforme dreigingsperceptie, dat wil zeggen dat verschillende betrokken partijen een andere perceptie kunnen hebben ten aanzien van dezelfde dreiging en er een andere lading aan geven vanuit die verschillen. Het is hierbij van belang te signaleren dat het in die beschrijvingen voornamelijk wetenschappers en experts zijn die bepalen wat de risico's zijn. *"Binnen deze rationele werkwijze blijkt weinig ruimte voor emoties en maatschappelijke onrust, terwijl hier in de samenleving wel grote behoefte aan is en het negeren hiervan in de praktijk grote negatieve consequenties kan hebben"* (De Graaf, 2013).

De gehanteerde dreigingsperceptie beïnvloedt de wijze waarop men vervolgens inzet op het tegengaan van de betreffende bedreiging (*veiligheidspraktijken*). Voor de legitimiteit van deze praktijken/maatregelen is het daarom van belang dat beleidsmakers geïnformeerd zijn over bestaande (verschillende) dreigingspercepties en deze zo goed mogelijk verdisconteren in de beleidsvorming en beleidsuitvoering.

2.6 VEILIGHEIDSPRAKTIJKEN EN -MAATREGELEN

Onder 'veiligheidspraktijken' en '-maatregelen' wordt het pakket aan acties en reacties verstaan dat doelbewust wordt ingezet in antwoord op de dreiging ter bescherming van de beschermwaardige waarden en belangen.

Als gevolg van de snel veranderende en grensoverschrijdende dreigingen wordt er steeds meer gedacht in termen van veiligheidsbeleid dat zowel de geografische-, de institutionele, als de grenzen van beleidsterreinen overbrugt. Middels deze integrale veiligheidsaanpakken tracht men om zo adequaat mogelijk op (potentiële) dreigingen te anticiperen (Stol et al., 2016).

Het advies van de WRR uit 2017 is hier een duidelijk voorbeeld van. De WRR geeft daarin aan dat het belangrijk is dat Nederland toewerkt naar een 'samenhangende strategie' tussen het buitenlandse en binnenlandse veiligheidsbeleid door middel van het oprichten van een

Algemene raad voor de veiligheid onder leiding van de premier, bestaande uit leden van de legertop en de ministers van Buitenlandse Zaken, Ontwikkelingssamenwerking en Veiligheid en Justitie. Ook pleit de WRR voor extra investeringen in de krijgsmacht. Beide adviezen zijn erop gericht de veiligheid van Nederlandse burgers te waarborgen.

In het regeerakkoord van het Kabinet Rutte III staat het volgende geschreven over het vernieuwen van veiligheidspraktijken (Regeerakkoord, 2017, p.3): "*Nederland is een democratische rechtsstaat die alertheid en onderhoud vergt om de vrijheid en veiligheid van burgers blijvend te kunnen waarborgen. Het zorgen voor een vrije, veilige en rechtvaardige samenleving is een kerntaak van de overheid. Voor een weerbare rechtsstaat is het belangrijk om mee te gaan met ontwikkelingen in de samenleving en de technologie. Hiervoor is het noodzakelijk dat wetgeving, beleid en de uitvoering hiervan worden gemoderniseerd. Ook zijn investeringen in de justitiële keten vereist. Er komen middelen voor meer menskracht en meer kwaliteit.*"

In de voortgangsbrief Nationale veiligheid staat te lezen (NCTV, 2016, p.1): "*Het kabinet speelt in op de veranderende situatie in de wereld en de voortschrijdende techniek. Het kabinet doet dit samen met alle partners in de veiligheidsketen. Veiligheid is een gezamenlijke verantwoordelijkheid van burgers, bedrijven overheden en maatschappelijke organisaties. We moeten nadenken wat ons handelen voor de korte termijn betekent voor de lange termijn. Dat is sturen in onzekerheid. Zo beschermen we onze samenleving en bewaren we het evenwicht tussen veiligheid en vrijheid.*"

Verder wordt meer dan in het verleden ingezet op internationale samenwerking. Zo heeft onder meer defensie de afgelopen jaren een voortrekkersrol gespeeld in de oprichting van baanbrekende vormen van samenwerking met internationale partners, waaronder *pooling and sharing* van capaciteiten.

Naast internationale samenwerking is in veiligheidspraktijken in toenemende mate sprake van samenwerking tussen publieke en private organisaties. Overkamp & Tollenaar (2013, p.78) deden onderzoek naar het integraal veiligheidsbeleid en planverplichting voor Nederlandse gemeenten en concluderen dat: "de toegevoegde waarde van het veiligheidsplan niet zozeer ligt in het plan zelf, maar in de procedure, waarbij partijen elkaar weten te vinden". Niet langer ligt de nadruk op de uitwerking van een uitgewerkt plan, maar veeleer is het van belang dat publieke en private partners met elkaar in contact staan en flexibel kunnen optreden in het geval van een dreiging.

Kortom, vanwege een veranderde kijk op (potentiële) dreigingen en veiligheid, ontstaat er een *veelheid* aan integrale veiligheidsplannen die de nadruk leggen op het slaan van bruggen tussen verschillende beleidsterreinen, landen en instituties. Hierbij gaat het vooral om ontkokering, flexibele samenwerking tussen verschillende netwerken van instanties en tussen publieke en private partijen, alsmede intensieve communicatie en informatie-uitwisseling.

In de landencasuïstiek (hoofdstukken 4 en 5) wordt gekeken op welke (integrale?) wijze de casuslanden hun veiligheidspraktijken rondom de betreffende dreigingen hebben georganiseerd. In hoofdstuk 6 wordt onder meer beschreven op welke manier Nederland kan leren van de integrale veiligheidsaanpak in Duitsland en Israël.

2.7 WOS: EEN 'BALANCEER ACT'

Het samenspel tussen de hierboven beschreven deelaspecten van de veiligheidscultuur bepaalt hoe een weerbare open samenleving omgaat met dreigingen. Het startpunt daarbij is vaak hoe een bepaalde dreiging gepercipieerd wordt, en door wie? Bij die dreigingsperceptie spelen de onderliggende waarden en belangen van de betreffende samenleving een belangrijke rol. De keuze voor de in te zetten veiligheidspraktijken wordt vervolgens bepaald door de wijze waarop naar de dreiging gekeken wordt en door wie en welke relatie, door wie, wordt gelegd, tussen de gepercipieerde dreiging en de onderliggende waarden en belangen.

Als gevolg van nieuwe en snel veranderende dreigingen komt er extra *spanning* te staan op het borgen van de balans tussen weerbaarheid en openheid. Zo bestaat het risico dat bij een stevige inzet op veiligheid, waar in het politieke discours met regelmaat op wordt aangestuurd, het middel erger kan worden dan de kwaal doordat er 'bijwerkingen' kunnen optreden voor een open samenleving. Zo worden bijvoorbeeld bevoegdheden van veiligheidsdiensten en politie bij dreigingen met regelmaat verruimd maar worden deze niet meer teruggedraaid bij afnemen van de dreiging (Noordegraaf et al., 2017).

2.8 TOEPASSING ANALYSEKADER

De wijze waarop samenlevingen omgaan met snel veranderende dreigingen en wat dit betekent in termen van het balanceren tussen de waarden en belangen van de open samenleving én de weerbaarheid ervan vormt de focus van dit onderzoek. We gaan in dit rapport inzichten ophalen uit situaties waarin ervaring is opgedaan in de omgang met een bepaalde dreiging, te weten het asiel- en migratievraagstuk in Duitsland en het *cybersecurity*vraagstuk in Israël (voor een nadere toelichting op de landenselectie zie hoofdstuk 3). Daartoe worden bij beide casus de kernconcepten van het analysekader besproken. Welke waarden en belangen wil men beschermen? Hoe wordt de dreiging gepercipieerd? Welke gevolg heeft dat voor de reactie op de dreiging en de ingezette veiligheidspraktijken? Welke partijen spelen hierin een rol en op welke wijze? Hoe verloopt het samenspel tussen beschermwaardige waarden en belangen, de dreigingsperceptie en de veiligheidspraktijken en welke afwegingen zijn er gemaakt tussen het streven naar weerbaarheid en openheid?

De casuïstiek levert daarmee inzicht in de praktijken en de bijbehorende afwegingen en de mogelijke consequenties ervan voor de samenleving en bouwstenen voor een toekomstvisie op weg naar een weerbare open samenleving. Hoe we deze lessen verzamelen en aan de hand van welke casuïstiek wordt beschreven in hoofdstuk 3, de onderzoeksopzet.

3. Onderzoeksopzet

3.1 OPZET OP HOOFDLIJNEN

Westerse samenlevingen worden geconfronteerd met uiteenlopende complexe dreigingen/verstoringen en ontwikkelen praktijken in een poging om hiermee om te gaan. Met dit onderzoek verzamelen we inzichten uit andere westerse landen over hoe omgegaan wordt met verschillende typen dreigingen voor de samenleving. Met de in hoofdstuk 2 beschreven conceptualisering van de veiligheidscultuur van 'weerbare open samenlevingen' wordt een analyse gemaakt van de wijzen waarop in twee uiteenlopende casus omgegaan wordt met dreigingen/verstoringen voor de weerbare open samenleving en wat Nederland hier mogelijk van kan leren.

3.2 GEBRUIKTE BRONNEN

Voor de beantwoording van de onderzoeksvragen maken wij gebruik van verschillende onderzoeksmethoden waarbij literatuurstudie en expertinterviews de basis vormen. De casuïstiek is uitgewerkt, gebruik makend van geschreven bronnen en expertinterviews. Vervolgens zijn de bevindingen uit de casuïstiek tegen het licht van de Nederlandse context bezien. Hiervoor is wederom gebruik gemaakt van geschreven bronnen en expertinterviews.

3.2.1 Literatuur en documentenanalyse

In de literatuurstudie is gebruikgemaakt van wetenschappelijke studies, kamerstukken en beleidsdocumenten die betrekking hebben op de weerbare dan wel open samenleving, het hedendaags veiligheidsdenken, de gepercipieerde dreigingen en op bijbehorende veiligheidspraktijken. Startpunt voor de zoektocht naar relevante studies waren literatuursuggesties van de betrokken onderzoeksexperts (prof. dr. Kees van den Bos, prof. dr. Beatrice de Graaf, prof. dr. Henk Kummeling, prof. dr. P. 't Hart en prof. dr. Mirko Noordegraaf).

Voor dit rapport is gebruikgemaakt van de onderstaande typen geschreven bronnen (voor zover beschikbaar):

1 Internationale en nationale *wetenschappelijke studies* over de weerbare open samenleving en veiligheidscultuur;
2 Internationale en nationale *rapporten en verslagen* over (potentiële) verstoringen en de anticipatie van de weerbare open samenleving op deze verstoringen;
3 Beleidsdocumenten en parlementaire teksten uit Duitsland en Israël met betrekking tot respectievelijk het asiel- en migratievraagstuk en de *cybersecurity* casus;

4 *Documenten van andere betrokken stakeholders zoals NGO's* met betrekking tot respectievelijk het asiel- en migratievraagstuk in Duistland en de *cybersecurity* casus in Israël;
5 *Nederlandse beleidsdocumenten en parlementaire teksten* met betrekking tot het asiel- en migratievraagstuk en de *cybersecurity*
6 *Documenten van andere betrokken stakeholders zoals NGO's* met betrekking tot het asiel- en migratievraagstuk en de *cybersecurity* in Nederland;

3.2.2 Expertinterviews

Bij het casusonderzoek en de vertaalslag naar de Nederlandse context is tevens gebruikt gemaakt van expertinterviews (zie Bijlage III voor een overzicht van de gesproken experts, en Bijlage IV voor de gehanteerde topiclijst).

- Reflectieronde met het UU-expertteam;
- Interviews met beleidsmedewerkers, medewerkers van betrokken overheidsdiensten en NGO's (indien beschikbaar) in de onderzochte landen;
- Een groepsinterview met private partijen in Israël;
- Interviews met veiligheidsdeskundigen, veiligheidsambtenaren, en publieke en private partijen die betrokken zijn bij het organiseren van veiligheid rondom het asiel en migratievraagstuk en *cybersecurity* in Nederland;
- Individuele toetsing van bevindingen bij UU-expert team.

Verder is in het kader van dit inventariserend onderzoek een masterscriptie geschreven door Berend Mutsaers, voor de master Publiek Management van de studie Bestuurs- en Organisatiewetenschappen van de Universiteit Utrecht. Het onderzoek met de titel *'Weerbaar door samenwerking? Een vergelijkend onderzoek naar triple-helix samenwerking bij innovatie op het gebied van cybersecurity in Nederland en Israël'* is tot stand gekomen binnen de context van en in nauwe afstemming met de onderzoekers van onderhavig inventariserend onderzoek. Delen van deze scriptie zijn, met toestemming van de auteur, opgenomen in H7 van dit rapport.

Opgemerkt dient te worden dat citaten uit interviews, literatuur en media, die vertaald zijn uit een andere taal dan het Nederlands, vertaald zijn door de auteurs van dit rapport.

3.3 CASUSSELECTIE

In dit onderzoek is een tweetal casus beschreven van westerse democratieën en hun omgang met een complexe, grensoverschrijdende dreiging/verstoring. Diversiteit van de casus was daarbij van belang om een breed continuüm aan verschillende inzichten op te kunnen halen. Om die reden is diversiteit van casuïstiek verkozen boven vergelijkbaarheid.

Verder was in de keuze voor de casuïstiek *ervaring* met een verstoring en de omgang ermee van cruciaal belang. In de geselecteerde *experienced cases* is beschreven hoe verschillende partijen (onder andere overheid, publieke en private organisaties, burgers) de verstoring percipiëren, welke belangen voor hen in relatie tot die specifieke verstoring beschermwaardig zijn en welke

maatregelen genomen zijn om de samenleving weerbaar te maken voor de desbetreffende verstoring. Met behulp van deze *experienced cases* kan geleerd worden van de maatregelen die zijn genomen om met de verstoring om te gaan. Op deze wijze kan de casuïstiek handvatten bieden voor het (verder) organiseren van weerbaarheid in een open Nederlandse samenleving. In de zoektocht naar diverse en experienced casus is in overleg met de begeleidingscommissie van dit onderzoek gekozen voor de volgende casuïstiek:

1 *Duitsland*: Omgaan met migrantenstromen
2 *Israël*: Afwending van *cyber*aanvallen

De Duitse casus is interessant vanwege zijn (initiële) openheid in de opvang van de grootschalige migrantenstroom die Duitsland als eindbestemming koos. In het recordjaar 2015 ving Duitsland meer dan 2,1 miljoen migranten op, waarvan de meesten Syrische vluchtelingen waren (Das Statistik Portal, 2017). Dit aantal was bijna een verdrievoudiging van de hoeveelheid migranten die Duitsland in 2010 (0,8 miljoen) welkom heette (Das Statistik Portal, 2017). Ondanks deze snelle en flinke groei van het aantal vluchtelingen dat gehuisvest moest worden, leek de Duitse regering in samenwerking met regionale overheden en publieke en non-profit organisaties, in eerste instantie goed in te kunnen spelen op deze migrantenstroom. De gekozen insteek leidt echter ook tot grote weerstand bij delen van de bevolking en de politiek en heeft daarmee stevige bij-effecten die de openheid en mogelijk ook de weerbaarheid van de samenleving onder druk zetten.

De Israëlische casus is interessant vanwege zijn weerbaarheid ten opzichte van *cybercrime*. Geen enkele ander natie heeft het afgelopen decennium zoveel geïnvesteerd in *cybersecurity*. Dit heeft ertoe geleid dat de Israëlische overheid en het Israëlische bedrijfsleven op grote schaal kennis en technische middelen exporteren naar andere landen en private organisaties om *cyber*aanvallen te herkennen en af te wenden (Forbes, 2017). Met behulp van een sterke privaat-publieke samenwerking op het vlak van *cybersecurity* stelt Israël zich heel weerbaar op ten opzichte van digitale aanvallen. De keuze voor deze casus suggereert echter niet dat Israel weerbaarheid op een voor Nederland wenselijke wijze combineert met democratische en rechtsstatelijke waarden. Israel laat volgens onder meer diverse internationale als Israëlische mensenrechten organisaties (Human Rights Watch, Amnesty international en de Israëlische NGO B'tselem) met regelmaat een beeld zien waarbij de democratische en rechtsstatelijke waarden onder druk staan. We zullen hier in dit onderzoek ook op terug komen. Deze casus geeft dan ook vooral inzicht in de mogelijke voor en nadelen van dit type veiligheidspraktijken in termen van een weerbare open samenleving.

Bij beide casus beschrijven we de verschillende deelaspecten van het analysekader en hun interactie. Zo wordt beschreven welke democratische en rechtsstatelijke belangen men beschermwaardig acht, en welk doel het weerbaar maken van de samenleving dient. Vervolgens wordt gekarakteriseerd met welke potentiële dreigingen de weerbare, open samenleving te maken heeft. Ten derde is beschreven tot welke nieuwe veiligheidspraktijken dit heeft geleid. Tot slot is beschreven hoe het zoeken naar de balans in de betreffende casus op het vlak van weerbaarheid en openheid gekenschetst kan worden.

3.4 VERTAALSLAG NAAR DE NEDERLANDSE CONTEXT

Vervolgens zijn de geleerde lessen vertaald naar de Nederlandse situatie. Daarvoor is een contextbeschrijving gegeven van de politieke en maatschappelijke discussie over de weerbare, open samenleving gebaseerd op recente verkiezingsprogramma's, ambtelijke documenten en krantenberichten. Vervolgens zijn de uit de casuïstiek geleerde lessen over (potentiële) dreigingen en veiligheidsmaatregelen getoetst bij soortgelijke Nederlandse organisaties, om tot verbeterimplicaties en aanbevelingen te komen.

4. De crisis rond de vluchtelingen-kwestie in Duitsland

4.1 INLEIDING

In deze casus wordt een beschrijving gegeven van de wijze waarop Duitsland is omgegaan met de grote aantallen vluchtelingen die vanaf 2015 richting Europa en vooral Duitsland kwamen. Gestart wordt met een beknopte beschrijving van de situatie en de betrokken actoren. Vervolgens wordt de aandacht gericht op de ervaren dreiging/verstoring en de belangen en waarden die verdedigingswaardig worden geacht, om daarna dieper in te gaan op de praktijken om deze waarden daadwerkelijk te verdedigen. De Duitse casus biedt inzicht in de complexiteit van het omgaan met deze grensoverschrijdende problematiek en de afwegingen die gemaakt worden wanneer getracht wordt recht te doen aan deels botsende belangen binnen een weerbare open samenleving.

4.1.1 De komst van vluchtelingen en de rol van Duitsland in 2015

Europa werd in 2015 geconfronteerd met een enorme vluchtelingenstroom die door media en politiek tot 'vluchtelingen*crisis*' werd bestempeld. Honderdduizenden vluchtelingen uit, in aflopende volgorde, Syrië, Afghanistan, Irak, Kosovo, Albanië, Pakistan, Eritrea, Nigeria, Iran en andere staten probeerden via de Balkan en de Middellandse Zee de relatieve veiligheid van Noordwest-Europa te bereiken (Eurostat, 2016).

Er was vooral een sterke toename van Syrische asielzoekers. De regering Assad liet haar burgers sneller vertrekken en de leefomstandigheden in opvangkampen in Libanon en Jordanië verslechterden door intrekking van subsidies uit Europa. Daarnaast maakte de regering van Macedonië met een nieuw transitvisum de doortocht naar het noordwesten gemakkelijker. De route Turkije-Griekenland werd daardoor aantrekkelijker (Sly, 2015).

Verschillende EU-lidstaten konden en wilden de vluchtelingen niet opvangen.

Met name Hongarije trachtte hen actief te weren. Vanaf medio juni 2015 begon het land met de bouw van grensbarrières. Begin september startte het bovendien pogingen om al aanwezige vluchtelingen terug te sturen naar de zuidoostelijke buurstaten. Ook andere landen beraamden stappen tegen de komst van immigranten. Een humanitaire catastrofe tekende zich af.

Duitsland vervulde in de vluchtelingencrisis een bijzondere rol. Geconfronteerd met het menselijk leed en de onmogelijkheid tot afdoende Europese afspraken te komen, nam bondskanselier Angela Merkel het heft in eigen hand. Aan de ene kant voerde haar regering in weerwil van het Schengenakkoord over vrij verkeer van personen tijdelijk opnieuw grenscontroles in (Oostenrijk, Slovenië, Hongarije, Zweden, Denemarken en niet-EU-lid Noorwegen volgden later dat jaar) (Eurostat, 2018).

Aan de andere kant opende Duitsland echter de grenzen voor vluchtelingen uit het buitenland. Sinds eind augustus 2015 paste de Duitse immigratiedienst de Dublin-procedure niet meer toe op Syrische vluchtelingen. Dat betekende dat zij niet meer naar het eerste EU-land van aankomst werden teruggezonden, maar dat hun asielaanvragen in Duitsland werden behandeld. Oostenrijk en Hongarije bekritiseerden deze maatregel, omdat ze een aanzuigende werking zou hebben.

Op 4 september 2015 besloot de Duitse bondskanselier Angela Merkel vervolgens in Hongarije gestrande vluchtelingen toe te staan via Oostenrijk naar Duitsland te reizen. Ze verklaarde dat het grondrecht op asiel ‘geen bovengrens’ kende. Wie bescherming zocht, kon die in Duitsland vinden. Het leidde tot een vrijwel ongekende toestroom van vluchtelingen naar haar land, niet alleen vanuit Hongarije. De op alle bestuurlijke niveaus reeds overbelaste overheidsorganen dreigden vervolgens te bezwijken onder de taak deze vluchtelingen op te vangen. Vele particuliere opvangorganisaties (ngo’s) en vrijwilligers schoten te hulp.

In totaal zouden in 2015 890.000 asielzoekers (*Schutzsuchenden*) naar Duitsland komen (Konar et al., 2017). Dit was een vervijfvoudiging vergeleken met 2014 (BAMF, 2015 In de jaren erna daalde het aantal jaarlijks nieuw aangekomen asielzoekers weer tot 280.000 personen in 2016 en 187.000 in 2017. Die daling zet zich vooralsnog in 2018 voort (BAMF, 2015).

De integratie van de asielzoekers stelt Duitsland voor een uitdaging. Hun sociaal-demografische kenmerken wijken opvallend af van de Duitse bevolking als geheel. Veel asielzoekers zijn jong (84 % is jonger dan 35 jaar) en mannelijk (60%). Meer dan de helft heeft vergeleken met de doorsnee Duitse bevolking een relatief laag opleidingsniveau (Bundesagentur für Arbeit, 2018). Zo’n driekwart van de asielzoekers die in 2015 en 2016 (eerste drie kwartalen) arriveerden, is moslim, 13 procent christelijk en 5 procent Jesidi (Konar et al., 2017).

4.1.2 Actoren

Een heel brede range aan overheidsorganisaties in de Bondsrepubliek, van het hoogste federale niveau via de instituties van de zestien deelstaten tot aan de lokale overheden was (en is) bij de opvang van vluchtelingen betrokken.

Voor dit onderzoek is gekeken naar drie overheidsdiensten die voor het complex immigratie en veiligheid een cruciale rol spelen.

Het BAMF (Bondsbureau voor Migratie en Vluchtelingen) Sinds de invoering van de nieuwe immigratiewet in 2005 heeft het BAMF onder meer tot taak asielaanvragen te behandelen en de integratie van vreemdelingen te bevorderen. Het BAMF ressorteert onder het Bundesministerium des Innern, für Bau und Heimat (Bondsministerie van Binnenlandse Zaken, Bouw en Heimat). Vanuit de BAMF-centrale in Neurenberg worden bureaus in alle zestien deelstaten aangestuurd. Omdat veiligheid een grotere rol is gaan spelen, kent het BAMF sinds 1 januari 2012 ook een Beratungsstelle Radikalisierung (adviespunt radicalisering) voor personen die zich zorgen maken over mogelijke radicalisering door een familielid of bekende. Deze Beratungsstelle heeft een belangrijke signalerende en preventieve rol.

Bundesamt c.q. *Landesämter für Verfassungsschutz* (BfV/LfV, de binnenlandse veiligheidsdiensten van Bond en deelstaten). Het gaat bij het Federaal Bureau c.q. de Deelstaatsbureaus voor de Bescherming van de Constitutie om de Duitse pendanten van de vroegere Nederlandse Binnenlandse Veiligheidsdienst (BVD: de huidige AIVD heeft ook een buitenlandse inlichtingentak). BfV/LfV ressorteren onder het Bondsministerie respectievelijk deelstaatsministeries van Binnenlandse Zaken. Hun taak is de preventieve verdediging van de grondwet en het daarop gebaseerde politieke bestel van Bond en de zestien deelstaten. In de Duitse grondwet uit 1949 en de daaruit afgeleide wetten over bijvoorbeeld politieke partijen en verkiezingen is expliciet vastgelegd dat de *freiheitliche demokratische Grundordnung* (FDGO, liberaal-democratische basisorde) in stand gehouden dient te worden.

De BfV/LfV moeten preventief gevaren voor de FDGO afweren door personen en organisaties, inclusief politieke partijen, die vermoedelijk tegen haar gekant zijn, te observeren en informatie over hen te verzamelen en aan bevoegde instanties ter beschikking te stellen. Indien nodig kunnen deze organisaties via een procedure bij het BVG worden verboden. Ook *Bundes*- en *Landeskriminalämter* (BKA en LKA, Federale en Deelstaatsrecherches) hebben overigens afdelingen die zich met politiek gemotiveerde criminaliteit bezighouden (zie hieronder).
BfV/LfV onderscheiden aangaande immigranten en vluchtelingen voornamelijk twee werkvelden: 1) Buitenlands extremisme (m.u.v. islamisme) en 2) Islamisme en Islamistisch terrorisme. Wat het eerste veld betreft, gaat het vooral om buitenlandse extremistische groeperingen die zijn voortgekomen uit politieke, sociale of etnische conflicten in hun landen van herkomst. Een voorbeeld vormt de Koerdische Arbeiderspartij (PKK), in Duitsland sinds 1993 verboden maar niet geheel verdwenen. De situatie op dit werkveld is min of meer stabiel (Bundesministerium des Innern, 2017).

Wat het tweede veld betreft, richt het BfV zich op groeperingen die de samenleving ondergeschikt willen maken aan een versie van de Islam die botst met de FDGO. Vooral de democratische basisbeginselen als de scheiding van kerk en staat, de volkssoevereiniteit, de gelijkstelling van man en vrouw en de religieuze en seksuele zelfbeschikking van het individu staan op het spel. Binnen het Islamisme vormen de Salafisten de meest radicale en dynamische stroming.

Onder hen bevinden zich 'jihadistische' Salafisten die hun doelen met geweld willen bereiken, mogelijk ook met terroristische aanslagen in Duitsland en andere westerse staten. *Bundeskriminalamt* c.q. *Landeskriminalämter* (BKA/LKA, de centrale recherchediensten van Bond en deelstaten). Deze Federale c.q. Deelstaatsrecherches, eveneens ressorterend onder de Bondsminster c.q. deelstaatministers van Binnenlandse Zaken, hebben onder meer tot taak de staat te beschermen door politieke gemotiveerde criminaliteit te bestrijden. BKA/LKA onderscheiden daarbij zes categorieën: politiek gemotiveerde criminaliteit van 1) linkse, 2) rechtse en 3) buitenlandse signatuur, 4) Islamistisch gemotiveerd terrorisme, 5) spionage en 6) volkenrechtsmisdaden (BKA, 2018). Bij 1-4 gaat het om strafbare handelingen waarbij het delict of de instelling van de dader(s) aanleiding geeft om te denken dat ze de democratische wilsvorming moeten beïnvloeden, zich tegen (aspecten van) de FDGO of het voortbestaan en de veiligheid van Bond of deelstaten c.q. de ambtsuitvoering door een lid van hun grondwettelijke organen richten, door geweld de buitenlandse belangen van de Bondsrepubliek willen schaden of gericht zijn tegen een persoon op grond van diens politieke overtuiging, nationaliteit, etniciteit, ras, huidskleur, religie, wereldbeschouwing, afkomst of uiterlijke kenmerken, handicap, seksuele oriëntatie of maatschappelijke status. Daarnaast richten BKA/LKA hun aandacht op strafbare handelingen die vallen onder specifieke wetgeving betreffende misdaden tegen de staat (BKA, 2018).

Naast deze instellingen verdient het Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK, Bondsbureau voor Bescherming Bevolking en Hulp bij Rampen) een korte vermelding. In 2015 speelde dit bureau, dat eveneens ressorteert onder het Bondsministerie van Binnenlandse Zaken, een essentiële rol in de praktische opbouw en organisatie van het coördinatiepunt van de Bond in München dat de vluchtelingen over de Bondsrepubliek distribueerde (KoSt FV-Bund) (BBK, 2018a). Een onderdeel van het BBK is het Gemeinsame Melde- und Lagezentrum (GMLZ) van Bond en deelstaten dat een breed scala aan overheidsorganisaties dagelijks informeert over eventuele nationale en internationale ontwikkelingen met implicaties voor de bescherming van de Duitse bevolking (BBK, 2018b). BAMF, BfV/LfV en BKA/LKA spelen echter voor de veiligheidsaspecten van asiel en migratie een veel centralere rol.

4.2 DREIGINGEN

De komst van een grote stroom vluchtelingen naar Duitsland leidt tot hevige reacties en een gepolitiseerde discussie over de wenselijkheid ervan. In deze paragraaf wordt geschetst welke reacties vanuit welke spectra van de samenleving te onderscheiden zijn en welke dreigingen gekoppeld worden aan de grote instroom van vluchtelingen.

4.2.1 Maatschappelijke en politieke reacties op de komst van de vluchtelingen

Hoewel de discussie over vluchtelingen in Duitsland in de laatste jaren vóór 2015 juist opvallend genuanceerd verliep, werd het thema 'asiel en migratie' al gedurende de eerste helft van 2015 steeds sterker gepolitiseerd.

Daarnaast was er sprake van een sterke toename van het aantal (brand)aanslagen op (geplande) asielzoekerscentra en fysieke aanvallen op (vermeende) vluchtelingen (BKA, 2015).
In reactie vormden zich ontvangstcomités die op diverse Duitse stations de net aangekomen vluchtelingen op een voor het oog van de wereld demonstratief uitgedragen Duitse *Willkommenskultur* onthaalden (Akrap, 2015).

Merkels opening van de grenzen (eerst als tijdelijke maatregel bedoeld) versterkte de politisering verder. Haar meermaals herhaalde motto *'Wir schaffen das'*, voor het eerst uitgesproken op een persconferentie op 31 augustus 2015, bleek olie op het vuur. Dit terwijl de Bondskanselier volgens sommigen juist dacht dat ze met die uitspraak met succes een appèl op de voor 2015 zo zichtbare nuancering van het vluchtelingendebat zou kunnen doen. Concrete politieke weerstand ondervond Merkel met name van de toenmalige Beierse minister-president Horst Seehofer van de aan haar eigen CDU verwante CSU. Deze eiste, uiteindelijk tevergeefs, dat ze alsnog een maximum aan de toestroom zou verbinden (Alexander, 2018).

Tegelijkertijd profileerde de relatief nieuwe, tot dan vooral Europa-sceptische partij *Alternative für Deutschland* zich als anti-immigratie en anti-Islam-partij. De AfD profiteerde daarbij van de mobiliserende werking van de protestbeweging Pegida (*Patriotische Europäer gegen die Islamisierung des Abendlandes*). In 2015 kwam het tot een felle uitbarsting van een al langer sluimerend conflict tussen tegengestelde visies op de Duitse nationale identiteit: zij die een terugkeer naar het traditionele narratief van een homogene natie wensten, botsten met degenen die waarschuwen voor de gevaren daarvan. Onder die laatsten bevinden zich ngo's als *Amnesty International* en *ProAsyl* die wijzen op de uit humanitaire overwegingen en afspraken over mensenrechten voortvloeiende morele plicht tot opvang van vluchtelingen. Opvallend genoeg schaarden zich echter ook meteen toonaangevende vertegenwoordigers van het Duitse bedrijfsleven achter het ruimhartige toelatingsbeleid. Zij beschouwden de komst van de migranten als een unieke kans voor Duitsland op economisch leiderschap in Europa (Arnold en Bischoff, 2016, pp.30-32).

Wellicht nog opmerkelijker was dat zelfs de massamedia enige tijd lang openlijk de kant kozen van de verwelkomers. De *Bild Zeitung* zette haar gebruikelijke campagnetoon in het najaar van 2015 tot verrassing van velen in tégen Pegida en de AfD en voor de hulp aan vluchtelingen. Twintig jaar eerder hadden vele toonaangevende media juist vooraan gestaan in het koor van de tegenstanders van de opvang van de toen vooral uit Joegoslavië afkomstige asielzoekers. Ze hadden daarmee forse steun gegeven aan de rechts-populistische partij *Die Republikaner* (Jakob, 2016, pp.9-10).

De gepolariseerde discussie rond vluchtelingen en migratie sinds 2015 is in hoge mate te herleiden tot een aanhoudend scherpe politiek-culturele strijd in Duitsland rond het thema asiel en migratie.

Hoewel het naoorlogse Duitsland eigenlijk voortdurend grote groepen migranten heeft opgenomen,[5] is het politiek vrijwel onverminderd controversieel gebleven om van Duitsland als immigratieland te spreken.
Dit terwijl de feiten eigenlijk daarvoor spreken, want van de ruim 82 miljoen Duitsers hadden in 2016 naar schatting 18,6 miljoen een migratieachtergrond (zelf of minstens een ouder uit het buitenland afkomstig) (BPB, 2018).

De late politieke natievorming (pas in 1871), de stormachtige historische ontwikkelingen in de twintigste eeuw, de controverses rond de 'verwerking' van het naziverleden en de naoorlogse Duitse deling en de na-ijlende verschillen tussen Oost en West zorgden ervoor dat het debat over wat Duits zijn inhoudt eigenlijk nooit in een duurzame consensus is uitgemond. Het integratiebeleid werd in Duitsland al vanaf de jaren tachtig een politiek omstreden thema. CDU en CSU en andere rechtse partijen speelden meermaals de integratiekaart. Kernthema's zijn het in 2000 door de CDU-politicus Friedrich Merz geïntroduceerde begrip *Leitkultur* – het idee dat immigranten zich moeten aanpassen aan een rond de Duitse taal en veronderstelde Duitse waarden, normen en gebruiken gesitueerde cultuur – en de notie *Parallelgesellschaften* – het idee dat naast elkaar bestaande, gescheiden gemeenschappen de samenleving als geheel ondermijnen (Tibi, 1996, pp.27-36).

Daarnaast waren er publicisten zoals Frank Schirrmacher (*Frankfurter Allgemeine Zeitung*) en Thilo Sarrazin (oud-SPD-politicus) die een verband legden met de relatief sterke vergrijzing van de 'autochtone' bevolking. Volgens hen zou een en ander leiden tot *Überfremdung* ('vreemde' culturen zouden de Duitse samenleving overspoelen) en verdringing door niet-westerse immigranten. Volgens Sarrazin trokken die laatsten het intelligentiepeil omlaag ten koste van Duitslands economische concurrentiepositie (Taberner, 2015, p.270).

De Islam werd al vroeg als een bijzonder cultureel obstakel voor integratie gezien, maar na 9/11 is dit vertoog enorm krachtig geworden. Symbolisch wordt de strijd over de integreerbaarheid van de Islam uitgedragen in debatten over onder meer het openlijk dragen van hoofddoeken, het ophangen van kruizen in scholen en rechtbanken (in Beieren), het losbandig en crimineel gedrag van migrantenkinderen in bepaalde stadswijken (zoals Neukölln in Berlijn) en een toekomstige EU-lidmaatschap van Turkije. De opstelling van politici is daarbij niet altijd eenduidig: Merkel nam zeer vroeg openlijk stelling tegen Turks EU-lidmaatschap, maar liet zich ook relatief positief uit over de plaats van de Islam in de Duitse samenleving. De politieke argwaan jegens de Islam correspondeert met de uitkomsten van opiniepeilingen waarin doorsnee Duitsers de Islam vooral met negatieve aspecten associëren (als benadeling van de vrouw, geweldbereidheid en fanatisme). Duitsers van Turkse afstamming noemen daarentegen juist positieve aspecten (als respect voor de mensenrechten, solidariteit, tolerantie en vredelievendheid) (Müller & Pollack, 2017, pp.41-46).

[5] Asielzoekers, gastarbeiders en etnische Duitsers uit de DDR en Oost-Europa en, via gezinshereniging, ook familieleden van deze drie groepen.

4.2.2 Koppeling van migratie en veiligheid in het politiek-maatschappelijk debat

Sinds 2015 zijn de discussies almaar feller gevoerd en spelen thema's als migratie en integratie een steeds grotere rol in verkiezingen op alle niveaus in de Bondsrepubliek. Ging het bijvoorbeeld bij de Bondsdagverkiezingen in 2013 volgens de kiezers nog vooral om sociale rechtvaardigheid, economisch - en arbeidsmarktbeleid, in 2017 lag de nadruk veel meer op de toestroom van vluchtelingen en binnenlandse en buitenlandse veiligheid (Statista, 2017).

Met name de AfD profiteerde hiervan, ook omdat 'integratie' symbool stond voor de vermeende incompetentie (en zelfs het 'volksverraad') van Bondskanselier Merkel. In de Bondsdagverkiezingen van 24 september 2017 haalde de AfD 12,6 procent van de stemmen en kon als derde fractie met 94 leden (van 709) tot de Bondsdag toetreden (Der Bundeswahlleiter, 2017).

Een cruciaal moment in de ontwikkeling van dit gepolariseerde politieke klimaat vormden de aanvallen op vrouwen door met name Noord-Afrikaanse migranten in de nieuwjaarsnacht 2015-2016 in Keulen (en enkele andere steden). Voor zover dat nog niet het geval was, was het thema 'asiel en migratie' in Duitsland vanaf dat moment ook in het brede politiek-maatschappelijke debat een *veiligheids*probleem geworden. Media als de *Bild Zeitung* die zich eerder enthousiast hadden opgesteld tegenover de *Willkommenskultur* gingen nu weer op afstand en echoden de nieuwe argwaan jegens de nieuwkomers. Dat de daders van 'Keulen' qua herkomst niet representatief waren voor de vluchtelingenstroom van 2015 maakte voor de omslag in het publieke debat geen verschil.

Die omslag werd vervolgens nog versterkt door de Islamistische terreuraanslagen in 2016 (in Duitsland een relatief nieuw fenomeen). Het tragisch dieptepunt daarvan was de grote moordaanslag met een vrachtwagen op de Kerstmarkt in Berlijn op 19 december 2016 (12 doden). Hoewel massapaniek uitbleef, droegen de aanslagen toch bij tot verdere ondermijning van de maatschappelijke cohesie.

Overigens koppelden politie en veiligheidsdiensten de vluchtelingenstroom al meteen in 2015 aan het vraagstuk veiligheid. In de eerste plaats rees bij het BKA bijvoorbeeld meteen de vraag wie er eigenlijk binnenkwamen en hoeveel criminaliteit de explosie van de aantallen immigranten met zich mee zou brengen. Men vreesde onder meer een vermeerdering en versterking van structuren van georganiseerde criminaliteit. Ook ging men ervan uit dat zich onder de vluchtelingen geradicaliseerde personen zouden bevinden en dat ISIS zou trachten terroristen Europa binnen te sluizen.

Toen in 2015 vele vluchtelingen naar Duitsland kwamen, richtten Islamisten hun werving op de nieuwkomers. Ook waren er aanwijzingen dat zich onder de vluchtelingen ook actieve en voormalige leden, ondersteuners en sympathisanten van terroristische groeperingen zoals ISIS bevonden, alsmede individuen met extremistische opvattingen en/of Islamistische oorlogsmisdadigers. Tegelijk maakte men zich ook op voor de terugkeer van de in eerdere jaren naar Syrië en Irak afgereisde Jihadisten (naar schatting 890 personen).

De BfV/LfV gingen de meldingen hierover stuk voor stuk na en wisselden daarvoor gegevens uit met andere diensten via het Gemeinsame Terrorismusabwehrzentrum (GTAZ) en Europese en internationale partners (Bundesministerium des Innern, 2016, pp.22-25).

In de tweede plaats was de veiligheid voor politie en veiligheidsdiensten al meteen in het geding wegens de explosieve toename van rechts-extremistisch geweld tegen veronderstelde vluchtelingen en opvangcentra en links-extremisme dat daarop volgde.
In 2015 nam het geweld tegen vluchtelingen en opvangcentra (vooral brandaanslagen, zie hieronder) enorm toe. Tegelijk was er sprake van grote agitatie tegen asielopvang die een legitimerende voedingsbodem voor dat geweld kan zijn en tot grote maatschappelijke polarisatie leidde. Ook politici, politieke activisten van andere politieke kleur en helpers van vluchtelingen werden soms aangevallen. Linkse extremisten reageerden met geweld tegen rechts (Bundesministerium des Innern, 2016, pp.9-11).
Het baarde de instanties daarbij zorgen dat relatief veel aanslagplegers opvallend genoeg geen rechts-extremistische voorgeschiedenis hadden. In 2018 deed zich, onder meer in augustus en september in de Oost-Duitse stad Chemnitz, een vergelijkbare vermenging van rechts-populisme en rechts-extremisme voor (BfV, 2018). Volgens de diensten wees dat erop dat rechts-extremistische radicalisering in bredere kringen van burgers om zich heen begon te grijpen. Sommige wetenschappers menen dat die analyse nog tekortschiet. In hun ogen is de categorie van rechts-extremistisch misleidend, omdat het geweld niet per se door die ideologie wordt ingegeven en ook niet van de rechterzijde van de maatschappij afkomstig is. Veeleer gaat het om ‘normale’ burgers die vinden de staat te weinig doet om de bestaande rechtsorde te beschermen (zoals zij die zien) en daarom zelf het heft in handen nemen. Het geweld tegen buitenlanders (en soms politici en activisten) is in feite een vorm van eigenrichting in naam van het volk. Dit ‘vigilantisme’ is overigens ook niet pas na ‘Keulen’ opgekomen, maar ontstond al in de jaren ervoor, bijvoorbeeld vanuit schijnbaar onschuldige burgerweergroepen (Quent, 2016, pp.20-21). Leden van een dergelijke groep, de Saksische ‘Bürgerwehr Freital/360’, werden in voorjaar 2016 op verdenking van terrorisme opgepakt en twee jaar later tot zware gevangenisstraffen veroordeeld (Spiegel, 2018).

4.2.3 Waarden

Als basiswaarde speelt een grote rol Duitsland zichzelf beziet als ‘streitbare’ c.q. ‘wehrhafte’ democratie, analoog aan de ideeën rond ‘militant democracy’ uit de jaren dertig van de sociaalwetenschappers Karl Loewenstein en Karl Mannheim. De overheid moet steeds bereid zijn om de liberaal-democratische basisorde (de FDGO) actief te beschermen. In de vroege Bondsrepubliek lag daarbij de nadruk sterk op het gevaar van overname van de staatsorganen door antidemocratische extremisten (‘waakzame’ democratie). Vanaf de late jaren zestig zette zich echter een visie door die de bescherming van de open samenleving vooropstelt en sterker redeneert vanuit de eerste 19 artikelen van de Grondwet over de grondrechten van de burgers (Rigoll, 2017, pp.40-41 en p.44). De kern staat in artikel 1.1: ‘De waarde van de mens is onaantastbaar. Haar te respecteren en te beschermen is de plicht van alle staatsmacht.’ (vertaling

door de auteur). Het *Bundesverfassungsgericht* (BVG, Federale Constitutionele Gerechtshof) heeft een serie basisprincipes van de FDGO vastgesteld.[6]
Meer concreet worden de waarden die men beschermwaardig vindt vooral zichtbaar in relatie tot de ervaren dreigingen en de wijze waarop de dreigingen worden gepositioneerd. In de discussie rondom asiel- en migratie in Duitsland worden vooral waarden als veiligheid, het gevoel van vrijheid en het vertrouwen in de overheid en de media naar voren gebracht.[7] Omdat het zoals gezegd vooral naar voren komt in relatie tot de ervaren dreigingen wordt hieronder ingegaan op deze waarden in relatie tot de ervaren dreiging.

De (zeer versterkte) koppeling van de thema's migratie en veiligheid is in Duitsland van relatief grote betekenis, omdat veiligheid in de politieke cultuur van het naoorlogse Duitsland vanouds een bijzondere plek inneemt. Zozeer zelfs dat de geschiedenis van de Bondsrepubliek wel als 'zoektocht naar veiligheid' is gekenschetst (Conze, 2009). De totale nederlaag en de grote verwoestingen waarmee het land zich in 1945 geconfronteerd zag, gekoppeld aan de traumatische ervaringen met mega-inflatie en economische depressie in de jaren twintig en dertig, zorgden aanvankelijk voor een politiek klimaat waarin het streven naar veiligheid – leven zonder angst om het leven en de bestaanszekerheid – centraal stond. Partijen spelen al decennialang in op deze veiligheidsgevoelens die leven in de samenleving (Frevel & Rinke, 2017). Veel Duitsers vertrouwen op een sterke, goed georganiseerde staat om de veiligheid en orde te garanderen. Het feit dat de Bondsrepubliek in 2015, geconfronteerd met de enorme toestroom van asielzoekers, niet in staat bleek c.q. niet volledig van zins was de eigen nationale grenzen te controleren, schokte dat vertrouwen in de staat echter diep – zo interpreteren althans sommige waarnemers de situatie.

Tijdens de laatste Bondsdagverkiezingen (2017) behoorden 'sicher' en 'Sicherheit' tot de meest gebruikte woorden in de verkiezingsprogramma's. Daarbij is 'veiligheid' in het politieke discours langzaam maar zeker getransformeerd van een voorwaarde voor de verwezenlijking van de grondrechten van de burgers tot een basiswaarde op zichzelf. Zo verklaarde de toenmalige Bondskanselier Gerhard Schröder (SPD) in 2002 dat zijn regering 'veiligheid' als 'elementair burgerrecht' beschouwde. Vijf jaar later sprak de CDU over veiligheid als een menselijke basisbehoefte (Conze, 2009).

Bij de koppeling van migratie aan veiligheid moet natuurlijk wel in acht worden genomen dat de meningen op dit punt zeer uiteenlopen.

---

6 Het gaat om: respect voor de in de grondwet concreet beschreven mensenrechten, met name het persoonlijke recht op leven en vrije ontplooiing; de volkssoevereiniteit; de scheiding der machten; de verantwoordelijkheid van de regering; de wetmatigheid van het bestuur; de rechterlijke onafhankelijkheid; het meerpartijenbeginsel; en de gelijkheid van kansen voor alle politieke partijen inclusief het recht op een grondwettige uitoefening van een oppositie. Zie: 'Freiheitliche demokratische Grundordnung', http://www.bpb.de/nachschlagen/lexika/pocket-politik/16414/freiheitliche-demokratische-grundordnung (geraadpleegd op 24 mei 2018).

7 Zoals hierboven aangegeven worden door sommige actoren ook andere belangen beschermwaardige geacht: zo wijst het bedrijfsleven op economische belangen, en ProAsyl op het belang van de bescherming van de veiligheid van vluchtelingen.

Zoals er een duidelijke en stabiele consensus ontbreekt over wat onder veiligheid moet worden verstaan, zo ontbreekt ook consensus over de waarden die door immigratie en het complex van daarmee samenhangende problemen en uitdagingen bedreigd zouden worden. Op basis van een brede studie in wetenschappelijke literatuur, persberichten en bronnen (zoals regeringsverklaringen, rapporten van politie- en veiligheidsdiensten, verkiezingsprogramma's van politieke partijen en opiniepeilingen) alsmede interviews met (vertegenwoordigers van) het BKA en het LKA Hessen, van het BAMF en van het *Institut für Demokratie en Zivilgesellschaft* ontstaat een beeld van die waarden en de achterliggende beschermwaardige belangen. Over twee categorieën van belangen leek daarbij consensus te bestaan, ongeacht de exacte invulling van de beschermwaardige belangen en de precieze bedreigingen en de implicaties voor het politieke beleid. Over een aantal andere heerste evenwel veel onenigheid tussen luide voor- en tegenstanders.

Ten eerste achtte men, bijna reflexmatig, de veiligheid van lijf en goed enigszins tot zeer bedreigd. Hierboven werd al vermeld dat ook een instantie als het BKA er vanuit ging dat door de stijging van het aantal asielzoekers het risico op terroristische aanslagen in het bijzonder en politiek gemotiveerd crimineel gedrag in het algemeen zou toenemen. Ook het risico op apolitieke vormen van criminaliteit (diefstal, geweldscriminaliteit etc.) schatte men hoger in. Bovendien ziet het BKA de laatste jaren eerste 'structuren' ontstaan tussen georganiseerde misdaad en terrorisme c.q. tegen de staat gerichte criminaliteit. Er lijken bijvoorbeeld Tsjetsjeense netwerken te bestaan met dienstverlening aan terroristen als *business model*. Ook dragen criminelen volgens het BKA bij aan de financiering van terrorisme door bijvoorbeeld te assisteren bij de illegale verkoop van geroofde cultuurgoederen uit het zogenaamde kalifaat van ISIS in Syrië en Irak.

Voor een deel geven de feiten dus wel aanleiding tot de angstige vermoedens: bepaalde soorten criminaliteit nemen door de komst van buitenlanders toe. Daarbij moet echter wel in aanmerking worden genomen dat sommige delicten alleen door buitenlanders gepleegd kunnen worden (zoals illegale grensoverschrijding). Ook zijn niet buitenlanders in het algemeen maar slechts enkele specifieke nationaliteiten in de criminaliteitscijfers oververtegenwoordigd. Het BKA ziet een groot onderscheid tussen wat ze humanitaire vluchtelingen noemt aan de ene kant en vluchtelingen uit Maghreb-staten (wier asielaanvraag vaak al is afgewezen) en Oost-Europese staatsburgers aan de andere kant. Vanuit de twee laatste groepen worden naar verhouding veel delicten gepleegd. De eerste groep was in aantallen echter veruit de grootste. Met andere woorden: de meeste 'echte' vluchtelingen jagen de criminaliteitscijfers volgens het BKA juist niet op.

Alleen al om deze reden is het verstandig om ook rekening te houden met de dominante beeldvorming over vreemdelingen en de dus minder op feiten gebaseerde argwaan die daaruit voortkomt. Bovendien tastten gebeurtenissen als de Oudejaarsnacht in Keulen het zelfbeeld van de westerse stad en stadsbewoner aan. De urbane liberaliteit en de daarmee verbonden levenskansen lijken op het spel te staan. De diffuse vrees voor de teloorgang daarvan wordt op de vreemdeling in het algemeen geprojecteerd (Münkler & Münkler, 2016, pp.73-77).

Het sinds 1992 jaarlijks herhaalde onderzoek naar de 'angsten van de Duitsers' door de R+V Versicherung toont aan dat in 2016 en ook daarna veel items in de angsten-top tien aan vreemdelingen gerelateerd waren. De uitslagen wijzen er echter ook op dat het wellicht minder de buitenlanders *an sich* zijn die de Duitsers angst inboezemden. Eerder de angst voor maatschappelijke spanningen door de migratiecrisis en twijfels aan het vermogen van bestuurders om die moeilijkheden op te lossen, scoren zeer hoog (R+V Versicherung, 2016).
In de ogen van velen zet de komst van vluchtelingen blijkbaar de maatschappij onder grote druk, het is als het ware een test die de samenleving moet doorstaan. Dat wekt deels irritatie over de vreemdeling in de hand, maar zet ook aan tot zelfonderzoek en verbetering van de eigen praktijken.

Dat neemt niet weg dat er ook op een tweede terrein een hoge mate van consensus bestond: algemeen gesproken achtte men bepaalde waarden en normen, met name de klassieke burgerlijke vrijheden en individuele vrijheidsrechten, door de komst van veel vreemdelingen bedreigd. In de voor dit onderzoek gehouden interviews en in commentaren in de media werd dit met name gearticuleerd aan de hand van vrouwenrechten, wat natuurlijk deels ook weer te herleiden is naar 'Keulen'.

Vaak werd de Islam als het achterliggende probleem beschouwd. Opvallend is daarbij de rol van enkele feministische wetenschappers en publicisten, zoals de antropologe Susanne Schröter, directeur van het *Frankfurter Forschungszentrum Globaler Islam* (FFGI) die ook advies geven aan overheidsinstanties. Schröter is bijvoorbeeld zeer kritisch over de rol van moskeeën bij de integratie van buitenlanders kunnen spelen, omdat ze in de praktijk plekken zouden zijn waar migranten de normen en gebruiken uit hun herkomstlanden conserveren (Schröter, 2016). Anderen menen dat moskeeën juist bruggen kunnen zijn naar cultuur en waarden van het 'land van aankomst' (Becker, 2018).

Er zijn ook categorieën van belangen die slechts door delen van de Duitse samenleving bedreigd en beschermwaardig worden geacht. Het gaat dan ten eerste om een veronderstelde Duitse nationale cultuur en identiteit. Deze wordt krachtig bepleit door met name de AfD, maar vindt ook bij een aanzienlijk deel van de Duitsers gehoor die niet op deze partij stemmen. Zij beschouwen immigratie als nationaal en/of cultureel risico. Ten tweede kan het gaan om Duitse economische belangen inclusief een toekomstbestendig economisch-demografische fundament voor verdere ontwikkeling van Duitsland. Hier zijn zowel tegenstanders als voorstanders van immigratie te vinden. Ten derde staat volgens eveneens een aanzienlijk groep Duitsers ook de acceptatie door de Duitse samenleving van andere culturen op het spel. Zij beschouwen immigratie meestal als kans, al zien velen ook in dat integratie niet vanzelf gaat. Ten vierde onderstreept een laatste groep van Duitse mensenrechtenorganisaties nog de veiligheid van vluchtelingen als beschermwaardig belang. Dit verwijst enerzijds naar het feit dat zij degenen zijn van wie de fysieke veiligheid zodanig in het geding was dat zij weg moesten vluchten uit hun land van herkomst. Met name ProAsyl wijst erop dat hun veiligheid in Duitsland een thema is dat vaak over het hoofd wordt gezien en dat via asielverlening beschermd zou moeten worden.

Anderzijds gaat dit punt ook over de veiligheid binnen de eigen vluchtelingen-gemeenschappen. Een respondent van ProAsyl wijst erop dat ook binnen deze gemeenschappen afpersing, onderdrukking en andere vormen van geweld voorkomen, soms onder invloed van trauma's.

Vooral bij overheidsdiensten en politiek lijkt ten slotte nog de inschatting aanwezig dat de vluchtelingenstroom als politiek-bestuurlijke uitdaging grote risico's met zich mee brengt voor het bestaande politieke bestel en daarmee de Duitse democratie. Allereerst constateren zij dat de politiek-maatschappelijke polarisatie enorm is toegenomen. Op de eerste plaats vrezen ze natuurlijk het geweld dat daaruit voort kan komen. Hierboven werd al gemeld dat rechts-extreem (en links-extreem) geweld in 2015 althans tijdelijk is toegenomen. In Hessen doorkruiste deze ontwikkeling bijvoorbeeld enigszins de in de jaren negentig ingezette pogingen om het politiekorps representatiever te maken door medewerkers te werven met een migratie-achtergrond. De toegenomen spanningen tussen migrantengemeenschappen en de bredere Duitse samenleving hebben de laatste jaren een doorwerking gekregen binnen de politie. Onderzoek naar een Turks-Duitse criminele organisatie werd enigszins gehinderd door argwaan jegens collega's met Turkse *roots* (Bundesministerium des Innern, für Bau und Heimat, 2018). Ook de verscherpte tegenstellingen onder bijvoorbeeld Turkse Duitsers over de politiek in Turkije, hebben hun effect op de verhoudingen binnen de politie. Het onderlinge collegiale vertrouwen is erdoor volgens het LKA onder druk komen te staan. Ook de Islam zorgt volgens een respondent van het LKA soms voor problemen, omdat mannelijke politieambtenaren hun vrouwelijke collega's geen hand (meer) willen geven.

Verder valt te constateren dat de polarisatie Duitsland kwetsbaarder maakt voor beïnvloeding van het Duitse politiek-maatschappelijke debat via *social media* door krachten van buiten. Hierdoor komt de betrouwbaarheid van berichtgeving onder druk komt te staan. Zij zien bijvoorbeeld dat Russische *fake news sites* al vroeg in 2016 kapitaal probeerden te slaan uit 'Keulen' door een volkomen verzonnen bericht te verspreiden over de verkrachting van een minderjarig Russisch-Duits meisje door drie mannen met Arabische achtergrond. Het was een evidente poging om de rond zes miljoen Duitsers met Russische wortels los te weken van de Duitse samenleving (Klimeniouk, 2016).

Bestuurders en beambten zien volgens diverse respondenten dat het vertrouwen in de overheid ondermijnd is door de vluchtelingencrisis. Analoog aan de hierboven aangehaalde angstpeiling heerst onder hen het beeld dat overheid en politiek in 2015 en 2016 in zekere zin voor een test stonden. Zij beseffen dat ze voor die test niet zijn geslaagd en ze realiseren zich dat het na de chaotische taferelen van die jaren geen sinecure is om het vertrouwen van de burgers terug te winnen. Verder geven diverse respondenten aan dat rechts-populisten juist rond de notie van *Staatsversagen* (overheidsfalen) een holistisch betoog hebben opgebouwd dat uit is op de de-legitimering van het bestaande politieke bestel en het fundament daarvan, de FDGO.

4.3 PRAKTIJKEN

4.3.1 FDGO als kader

De liberaal-democratische basisorde (FDGO) biedt een helder kader voor waar het bij de verdediging van democratie en rechtsstaat concreet om gaat (zie 4.2.3 Waarden).

Uit de interviews en de literstuurstudie voor het onderhavige onderzoek is de indruk verkregen dat politici en leidinggevende bestuurders zich terdege bewust zijn van dit kader. Maar op de meer uitvoerende niveaus lijkt het FDGO veel minder expliciet aanwezig. Zo wordt er in de dagelijkse (overleg)praktijk nauwelijks naar verwezen. BKA'ers verwijzen bijvoorbeeld gewoon naar het Strafrecht en het Strafprocesrecht als het kader voor hun functionele doen en laten. Wel speelt de FDGO volgens het BKA bij de opleiding en ambtsinvulling van alle ambtenaren steeds een expliciete rol. *BAMF*- vertegenwoordigers verklaarden daarnaast dat de FDGO richtinggevend voor hun handelen is.

4.3.2 Verzamelen en delen van informatie

Onder de maatregelen binnen het complex van migratie en veiligheid valt allereerst op dat de Duitse overheid sterk heeft ingezet op de verbetering van de informatiepositie over de binnenkomende migranten. Alle bij veiligheid betrokken diensten werken als het gaat om de dreiging van terrorisme al jaren samen in verbanden als het in 2004 opgerichte Gemeinsame Terrorabwehrzentrum (GTAZ) en het in 2012 begonnen, meer op extremistisch politiek geweld gerichte Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ).[8] In de tweede helft van 2015 deed zich echter het probleem voor dat het de Bundespolizei en het BAMF niet meer lukte om alle asielzoekers zo snel mogelijk te registreren en in de asielprocedure te leiden. Niet alleen ontbraken daardoor de precieze aantallen, maar ook allerlei andere gegevens op individueel niveau. In september 2018 kreeg het BKA de taak om een extra inspanning te leveren voor het verzamelen van cijfermatige gegevens om toch een inschatting te kunnen maken van de criminaliteit die wellicht in samenhang met de immigratie zou ontstaan.

Het BKA stuitte daarbij op een voorspelbaar Duits probleem: het federalisme. De afzonderlijke politieorganisaties van de zestien deelstaten, de douane en de *Bundespolizei* hebben alle hun eigen statistische programma's om bijvoorbeeld delicten en daders te registreren. Als een politieagent wil weten welke informatie verschillende deelstaatspolitieorganisaties hebben verzameld over een verdachte, dient hij eigenhandig in al die systemen te (laten) zoeken. Zoals een van de gesprekpartners van de Duitse politie al opmerkte, moet dat dan wel een slimme en ambitieuze agent zijn die goed in staat is de verschillende systemen te doordringen en inlichtingen daaruit aan elkaar te koppelen.

---

[8] Deze coördinatiecentra zijn nodig om in Duitsland, met zijn strikte scheiding tussen politie en veiligheidsdiensten en zijn federale structuur, tot een optimale uitwisseling van informatie te kunnen komen binnen de wettige kaders.

In de aanloop naar de aanslag in Berlijn bleef in IT-systemen aanwezige informatie over de dader onbedoeld onbenut, met alle gevolgen van dien.[9]

Toevallig hadden Bond en deelstaten kort voor die aanslag wel al besloten tot het Saarbrücker Programm, dat onder meer de ontwikkeling van een nieuwe overkoepelende en federale IT-'architectuur', *Polizei 2020*, inhoudt (Bundesministerium des Innern, für Bau und Heimat, 2018). Of de nieuwe IT-architectuur werkelijk een succes wordt, moet worden afgewacht. In elk geval is de benodigde vernieuwing van de federale wetgeving over de BKA, inclusief de omgang met persoonsgebonden data door de politie, inmiddels afgerond. De Duitse politievakbond DpolG (2018) blijft echter kritisch over de hardnekkigheid waarmee sommige deelstaten aan eigen IT-systemen vast lijken te houden.
Los van de creatie van die nieuwe federale IT-architectuur werden sinds 2015 ook al stappen gezet richting de centrale verzameling en analyse van gegevens over vluchtelingen. Onder regie van het BKA is het gelukt om te komen tot gezamenlijke *Lageberichte* (situatieschetsen) in een reeks van categorieën, zoals georganiseerde criminaliteit, wapens en drugs. Met behulp van softwareontwikkelaars is op basis van moeizaam vastgestelde gezamenlijke criteria een nieuw systeem ontwikkeld. Die verbeteringen hebben in elk geval al geleid tot goede gezamenlijke jaarcijfers over opgeloste misdaden in de gehele Bondsrepubliek (de dagelijkse systemen zijn nog altijd zeer verschillend). Zonder de vluchtelingencrisis was de doorbraak er wellicht niet gekomen, want in normale situaties houden de *Länder* volgens een van de respondenten liever vast aan de eigen autonomie.

In diezelfde sfeer van informatieverzameling vallen ook allerlei kwalitatieve verbeteringen in de administratieve procedures van het BAMF rond asielaanvragen. Inmiddels slaagt die dienst er naar eigen zeggen in de identiteit van asielzoekers goed en snel vast te stellen. Identiteitsbewijzen worden op echtheid gecontroleerd, vingerafdrukken en andere biometrische gegevens worden verzameld en er worden pasfoto's gemaakt. Deze gegevens worden gedeeld met andere overheidsorganisaties via een *Kerndatensystem* (IT-systeem met sleutelgegevens) dat eerdere deelstaatssystemen heeft vervangen. Daarnaast speelt veiligheid en criminaliteit een veel grotere rol in de *Befragung zu den Fluchtgründen* (in IND-termen: de 'gehoren' over de vluchtredenen). Gespreksverslagen worden veel meer geanalyseerd op voor veiligheid relevante informatie. Bovendien zijn er aan de standaardvragen voor de 'gehoren' ook extra vragen uit de koker van de politie en veiligheidsdiensten toegevoegd. Kortom, de intensiteit en kwaliteit van de samenwerking met andere diensten is volgens het BAMF duidelijk toegenomen.

Ook enkele organisatorische verschuivingen binnen het BAMF sinds 2015 wijzen er overigens op dat de aandacht van het bureau voor de veiligheidsaspecten van asiel en immigratie gestegen is.

---

[9] Het ging onder meer om zo'n zeven weken vóór de aanslag bij het LKA Berlijn bekend geworden informatie dat de bewuste Tunesiër Anis Amri in drugs handelde. Op grond daarvan had hij naar zijn land van herkomst kunnen worden teruggestuurd. Zie: Eckart Lohse en Markus Wehner, 'Missglückte Vertuschung. Der Fall Amri', *Frankfurter Allgemeine Zeitung*, 18 mei 2018.

Zo toont het organogram van het BAMF sinds 1 oktober 2018 een aparte afdeling (*Abteilung 7*) die zich bezighoudt met Sicherheit im Asylverfahren. Deze sectie heeft onder meer bureaus (Referate) voor *Grundsatz Sicherheit im Asylverfahren* (principiële vragen aangaande veiligheid in de asielprocedure) en *Operative Zusammenarbeit mit den Sicherheitsbehörden des Bundes und der Länder* (operatieve samenwerking met de veiligheidsdiensten van Bond en deelstaten). Ook de eerder in paragraaf 4.1 genoemde *Beratungsstelle Radikalisierung* is als bureau bij de nieuwe sectie ondergebracht.[10]

Ten slotte is zeker ook sprake van voortschrijdende internationale samenwerking als het gaat om het verzamelen en delen van informatie. De Islamistische terreuraanslagen in Europa, met name die in Parijs in 2015, hebben duidelijk laten zien dat organisaties als ISIS internationaal opereren. Ook leeft onder politie en veiligheidsdiensten sterk het besef dat vrijwel alle gevallen van zware criminaliteit internationale aspecten bezitten. De samenwerking met Europol en Interpol is toegenomen, maar kent ook grenzen. Aan de ene kant komt dat door moeilijkheden over de aansluiting van verschillende nationale systemen op elkaar, een soort uitvergrote versie van de problemen die er op federaal niveau binnen Duitsland al zijn. Aan de andere kant gaat het volgens de vertegenwoordiger van het LKA om de vraag of het politiek wenselijk en juridisch toelaatbaar moet worden geacht informatie met andere landen te delen, zeker als de praktijk van politie en justitie er niet voldoen aan Europese standaarden. Zo kan bijvoorbeeld bekend zijn dat verdachten in een bepaald land vaak aan marteling blootstaan; uitwisseling van informatie kan dan strijdig zijn met respect voor mensenrechten.

4.3.3 Aanscherping asielrecht en andere wetgeving

Op het gebied van wetgeving is in reactie op de vluchtelingenstroom in Duitsland sinds 2015 een groot aantal aanpassingen doorgevoerd in het asielrecht en in aanverwante regelingen. Daartoe behoort onder meer een beperking van de bewegingsvrijheid van een asielzoeker zonder status. Zo'n *Geduldete* (gedoogde) mag in de eerste drie maanden de deelstaat waar hij (op aanwijzing van de overheid) verblijft niet zonder toestemming verlaten. Die termijn kan sinds 2016 worden verlengd als de asielzoeker wegens een misdaad is veroordeeld (behalve als hij het vreemdelingenrecht heeft overtreden), als hij wordt verdacht van overtreding van de wet op verdovende middelen of als hij binnen afzienbare tijd het land moet verlaten (ProAsyl, 2016).

Daarnaast kunnen afgewezen asielzoekers sinds mei 2017 sneller worden uitgezet en in afwachting daarvan gedetineerd, bijvoorbeeld als hard kan worden gemaakt dat er van hen mogelijk ernstig gevaar uitgaat voor lijf en leven van derden of voor de binnenlandse veiligheid in het algemeen (Deutscher Bundestag, 2017).

Al met al zijn de vernieuwde asielwetten de restrictiefste die de Bondsrepubliek sinds de oprichting in 1949 ooit heeft gehad. Bovendien kunnen andere wetten nog tot verdere verscherping van de omstandigheden leiden.

---

[10] Vergelijking van BAMF-organogrammen uit 2015, 2016 en 2017, via de website (en oude versies daarvan).

Vrijwel alle deelstaten – Beieren gaat daarin voorop met de extreemste verscherping – hebben inmiddels een nieuw *Polizeiaufgabengesetz* (wet over de taken van de politie). Deze wetten kennen een enorme uitbreiding van de bevoegdheden van de politie en perken de burgerlijke vrijheden danig in. De politie mag bijvoorbeeld eerder beginnen een persoon 'in de gaten te houden' (al bij 'dreigend' en niet pas bij een 'concreet' gevaar). Er hoeven dus nog geen strafbare feiten te zijn gepleegd.

Los van deze politiewet werd in Beieren in juli 2017 al het voorarrest vergemakkelijkt. Potentiële daders kunnen preventief vastgehouden tot een termijn van drie maanden, waarna een rechter over verlenging moet beslissen, zonder dat een hoogst aantal verlengingen is vastgelegd (vroeger waren dat twee weken) (Schnell, 2018). Grote protesten tegen de verscherping van de politiewet haalden uiteindelijk niets uit.

In het verlengde van eerdere verboden van Salafistische organisaties, sprak toenmalig Bondsminister van Binnenlandse Zaken Thomas de Maizière (CDU) op 25 oktober 2016 opnieuw een verbod uit. Dit keer betrof het de Islamistische dawa-organisatie 'Die Wahre Religion' (DWR) en haar Koran-verspreidingsactie 'Lies!'. Al sinds 2011 deelden DWR-activisten vanachter *stands* in winkelstraten Korans uit en spraken met geïnteresseerden over de Islam. Toen duidelijk was geworden dat het hen om rekrutering voor de jihad ging, besloten de autoriteiten tot het verbod.[11]

4.3.4 Publieksgerichte beleidscommunicatie

Waren bovengenoemde maatregelen gericht tegen mogelijke, direct door vluchtelingen veroorzaakte veiligheidsproblemen, uit beleidsstukken en interviews wordt ook duidelijk dat de Duitse overheid probeert een oplossing te vinden voor de publieke polarisatie rond het thema migratie en veiligheid. Politici en bestuurders zijn volgens diverse respondenten veel meer aandacht gaan besteden aan de communicatie over het betreffende beleid. Het is niet altijd meteen te relateren aan de recente vluchtelingencrisis, maar het lijkt volgens een respondent van het LKA gebruikelijker te worden dat leidinggevenden een intensieve werkrelatie met de voor hen relevante lokale, regionale of landelijke media onderhouden.

Ook lijkt men (nog) meer dan vroeger open te staan voor de gedachtewisseling met wetenschappers en zoekt men nadrukkelijker het directe contact met de burgers, met name door intensief gebruik van *social media* zoals twitter. Volgens Matthias Quent van het *Institut für Demokratie und Zivilgesellschaft* presteert de politie daar door de bank genomen echt goed en bereikt zelfs een hoge graad van interactie, waardoor er een zekere resonantie in en een binding met de bevolking is ontstaan. Al neemt dat niet weg dat er nog steeds negatieve uitzonderingen van publiciteitsschuwe gezagsdragers voorkomen en dat er nog altijd niets gaat boven goede contactambtenaren ter plekke in problematische wijken en regio's.

---

[11] Bundesministerium des Innern, Verfassungsschutzbericht 2016. Fakten und Tendenzen – Kurzzusammenfassung (Berlijn, z.j. [2017]), 26.

Om weerstand te bieden tegen de feitenloze informatie die onder meer via *social media* haar weg naar het publiek vindt, is het BKA er in 2016 mee begonnen kwartaal- en jaarrapporten te publiceren over 'Kriminalität im Kontext von Zuwanderung' (criminaliteit in de context van immigratie). De gedachte was dat men het publiek kon helpen weg te komen van de emoties rond het thema door de simpele feiten onder de aandacht te brengen. Dat was nog geen sinecure, want daarvoor was het eerst nodig de informatievergaring door de verschillende diensten te stroomlijnen, aldus het BKA.

Het BKA nam een risico met rapporten over het verband tussen criminaliteit en immigratie; extreme groeperingen konden hier gemakkelijk mee op de loop gaan. Toch duidde de ontvangst in mei 2018 van het meest recente jaarrapport erop dat wel degelijk bepaalde nuances door grote dagbladen als *Die Welt* en *Bild Zeitung* werden overgenomen. Volgens *Bild Zeitung* sprak van 'verrassende feiten', zoals dat vluchtelingen uit burgeroorlogsgebieden naar verhouding minder vaak betrokken waren bij misdaden (Weise, 2018).

Een kritische wetenschapper als Quent kan de inspanningen van het BKA dan ook waarderen als een eerlijke poging het debat op een meer feitelijke basis te stellen. Volgens Quent is de intentie achter die BKA-rapporten goed en was het ook nodig om iets te stellen tegenover de sfeer van verdoezeling van misstanden en falen die soms heerste, bijvoorbeeld rond 'Keulen', waar de politie maar langzaam met de feiten uit de bewuste nacht kwam. Hij meent wel dat de overheid als geheel nog meer kan streven naar gecoördineerd communicatiebeleid met helder omlijnde strategische thema's die ook werkelijk nagestreefd worden. Te vaak regeert in zijn ogen nog de waan van de dag, wat vooral betekent dat politici hun thema's ongewild laten dicteren door de AfD en zich laten opdrijven door de percentages van die partij in verkiezingen en opiniepeilingen (Quent, 2016).

4.3.5 Heimat-beleid als symbolisch antwoord op de zorg over integratie

Achter dat communicatiebeleid gaat de gedachte van politici, bestuurders en beambten schuil dat men wellicht toch te weinig naar de doorsnee Duitser had geluisterd – het is een reflexmatige reactie op de electorale doorbraak van de AfD die vergelijkbaar is met die van de Nederlandse politiek na de Fortuyn-revolte. In juni 2018 leidde die reflex zelfs tot een crisis binnen de christendemocratie in Duitsland rond de vraag of asielzoekers aan de grens tegengehouden mochten worden of niet. In het kader van een nieuw 'masterplan' over immigratie wilde minister van Binnenlandse Zaken Seehofer daartoe overgaan, zelfs nadat Merkel, net als in 2015, had verklaard daartegen te zijn. Zo dreigde de pas begin 2018 aangetreden Bondsregering alweer te vallen door strijd tussen de Beierse CSU (voorzitter Seehofer) en de grotere zusterpartij CDU (voorzitter Merkel) (Braun & Fried, 2018). Uiteindelijk kwam er een compromis uit de bus dat voorzag in kortstondige opname van asielzoekers met weinig kansen op toelating in centra direct aan de Duits-Oostenrijkse grens.

Het is duidelijk dat Seehofers voorstel verband hield met de verkiezingscampagne in Beieren, waar de CSU voortdurend gestes doet naar potentiële AfD-kiezers onder haar eigen stamelectoraat.

Het nieuwe migratiemasterplan was echter niet de enige methode waarop Seehofer dat probeert. Tot zijn toolbox behoort ook een nieuw beleidsterrein, *Heimat*, dat op aandringen van de CSU onlangs is toegevoegd aan de verantwoordelijkheden van het Bundesinnenministerium. Het lijkt een symbolische tegemoetkoming aan de Duitsers die zich zorgen maken over de globalisering en de komst van vluchtelingen en daarin een bedreiging zien voor de Duitse nationale identiteit. Het is nog zeer diffuus wat Seehofer en zijn CSU met dat beleidsterrein werkelijk van plan zijn. In elk geval lijken ze te willen voorkomen dat alleen de AfD dat thema mag invullen. Als regionale partij wil de CSU dat niet laten gebeuren – in Beieren zelf bestaat ook al sinds 2014 een Heimat-ministerie. In het buitenland werd het initiatief ook meteen begrepen als een omhelzing van identiteitspolitiek, wat ook wel gerechtvaardigd werd door uitlatingen van prominente CSU'ers over de onverenigbaarheid van de Islam met westerse waarden (The Economist, 2018). Seehofer (2018) zelf heeft in een lang ingezonden artikel in de *Frankfurter Allgemeine Zeitung* eind april 2018 juist een heel open, bijna sociaaldemocratische visie op Heimat-beleid gegeven. Het voornaamste wapenfeit van het Beierse Heimat-ministerie is ook vrij onschuldig: door haar inspanningen wordt binnenkort de laatste afgelegen boerderij door aansluiting op het glasvezelnet met de wereld verbonden (Knopp, 2018).

Kritiek op het Heimat-beleid lijkt kortom nog wat vroeg, maar de al eerder aangehaalde Quent stelt terecht de vraag of het zo verstandig is zo'n diffuus begrip als kapstok voor beleid te gebruiken. De kans is groot dat iedereen daar zijn eigen hoop en verwachting op projecteert, waardoor teleurstellingen bij de burgers als het ware voorgeprogrammeerd zijn.

4.3.6 Het optreden van de overheidsactoren

Samen met de Bundespolizei, die geacht wordt binnenkomende migranten aan de grens te registeren en deze taak in 2015 nauwelijks kon vervullen, stond vooral het BAMF onder grote druk. Het ontbrak aan personeel om met de geboden snelheid de nieuwkomers te horen over hun asielgronden en een voorlopige beslissing te nemen (meer dan de helft van hen kon pas in 2016 worden gehoord). Tijdelijk aan andere overheidsdiensten (Bundespost, Bundesagentur für Arbeit, Bundeswehr etc.) onttrokken personeel kon slechts in beperkte mate soelaas bieden, mede door gebrek aan de benodigde specialistische kennis en ervaring.

Dit leidde tot grote fouten, zoals in de zaak-Franco A. Een rechts-extremistische *Bundeswehr*-officier beraamde met enkele gelijkgestemde medeplichtigen een plan om zich voor te doen als asielzoekers en een aanslag te plegen om zodoende vluchtelingen in diskrediet te brengen. Hij slaagde er eind 2016 in als Syrische asielaanvrager geregistreerd te worden. De basis voor die erkenning was een in het Frans (in plaats van Arabisch) gevoerd gesprek met een tijdelijke BAMF-medewerker (van de Bundeswehr). Het BAMF zag in deze zaak aanleiding om tweeduizend asielaanvragen opnieuw te controleren (Deutscher Bundestag, 2017).

Mogelijk heeft de hectiek van 2015-2016 ook gelegenheid geboden aan BAMF-medewerkers om in asielzaken eigenmachtig positieve beslissingen te nemen, wellicht tot eigen voordeel.

Voorjaar 2018 dat er in bepaalde situaties talrijke onregelmatigheden waren in het BAMF-deelstaatsbureau in Bremen. De net aangetreden bondsminister van Binnenlandse Zaken Horst Seehofer (CSU) stelde een onderzoek in, verving de directeur van het BAMF en zette een reorganisatie in gang (Van de Poll, 2018). In de nazomer van 2018 werd steeds duidelijker dat er, anders dan aanvankelijk gedacht, uiteindelijk in slechts in 1 % van de afgehandelde asielverzoeken ten onrechte positieve besluiten waren genomen en dat alleen in één van de zestien BAMF deelstaatsbureaus.

Tijdens de vluchtelingencrisis van 2015 richtten BKA/LKA zich in het bijzonder op politiek gemotiveerde criminaliteit van rechterzijde (wegens de brandaanslagen op asielzoekerscentra e.d., zie hieronder) en op politiek gemotiveerde criminaliteit door buitenlanders en islamistisch gemotiveerd terrorisme.

Vooral bij die laatste categorie is het een belangrijk instrument van het BKA of de deelstaatspolitie om bepaalde personen tot *Gefährder* (bedreiger) of *Relevante Person* (ondersteuner) te bestempelen en ze daarna nauwgezet te volgen. Als *Gefährder* worden personen beschouwd van wie feiten bekend zijn die het aannemelijk maken dat ze zwaardere politiek gemotiveerde delicten zullen plegen.
Gefährder en *Relevante Person* zijn begrippen die op zichzelf niet juridisch gedefinieerd zijn, maar uit de politiepraktijk sinds 9/11 voortkomen. Door de catastrofale impact van de aanslagen in de VS hechtte ook de politie (en niet enkel de veiligheidsdiensten) veel meer waarde aan het vroegtijdig herkennen van gevaren. Dat uitte zich in een verscherpte focus op het extremistische milieu van eventuele daders. Vanaf 2002 wordt naar bepaalde personen systematisch onderzoek gedaan om te kijken of ze als *Gefährder* of *Relevante Personen* bestempeld moeten worden. *Gefährder* worden vaak op de hoogte gebracht van hun status, wat intimiderend werkt. Critici zien het gevaar van willekeur en voorveroordeling (Kretschmann, 2017).

Het BKA heeft de centrale regie inzake *Gefährder* in handen en voert de systematische analyse en inschatting van de indicaties en feiten alsmede de prognostiek over *Gefährder* uit. Het werkt daarbij nauw samen met de politie- en veiligheidsdiensten op Bonds- en deelstaatsniveau, onder meer binnen de gemeenschappelijke centra voor terreurbestrijding, zoals het GTAZ.
Inmiddels is het aantal *Gefährder* opgelopen tot 745 en telt men 457 relevante personen (stand 6 februari 2018, een jaar tevoren ging het nog om resp. 570 en 360). Om dat grote aantal te kunnen managen, gebruikt het BKA sinds 2017 nieuwe software om op individueel niveau de risico's te kunnen inschatten. Dit instrument, RADAR-iTE geheten, is in samenwerking met de Arbeitsgruppe Forensische Psychologie van de Universität Konstanz ontwikkeld (Deutscher Bundestag, 2018).

Het ligt ook in de bedoeling van de overheid om migranten zonder of met een tijdelijke verblijfsstatus die als *Gefährder* zijn bestempeld (of anderszins als crimineel gelden) terug te sturen naar hun land van herkomst of een transitland. De aanscherping van de asielwetgeving in mei 2017 was deels ook bedoeld om dit uitzetten gemakkelijker te maken, maar in de praktijk staat een complexe rechtsgang de snelle uitzetting nog altijd in de weg.

4.3.7 Het optreden door niet-overheidsactoren

Het beeld zou niet compleet zijn zonder een indruk te schetsen van de vele burgerinitiatieven die in Duitsland plaatsvinden en die onder andere gericht zijn op de opvang van asielzoekers en vluchtelingen.

Ook deze hebben invloed op percepties van dreigingen en ze zijn uitingen van achterliggende waarden die volgens sommige groepen bescherming verdienen.
Zij maken ook duidelijk dat de *Wilkommenskultur* nog wel degelijk sterk aanwezig is in de Duitse samenleving.

Dit soort initiatieven wil enerzijds de sociale en economische integratie van vluchtelingen bevorderen als bescherming van de waarde van de liberaal democratische rechtstaat. Meer specifiek gaat het om het aspect van het beschermen van de mensenrechten. Die wordt enerzijds nauw opgevat, als zijnde de bescherming van leven en vrijheid van vluchtelingen die naar Duitsland zijn gekomen. Maar anderzijds wordt deze ook breder ingevuld, in lijn met het Vluchtelingenverdrag, namelijk dat vluchtelingen ook recht hebben op het kunnen voorzien in hun levensonderhoud, bijvoorbeeld via werk. Ook op indirecte wijze wordt de waarde van veiligheid via deze burgerinitiatieven beschermd. Zij hebben als achterliggende aanname dat integratie het beste instrument is om veiligheid te bewaken omdat zij betrokken inwoners creëert en radicalisering tegengaat, aldus een respondent van Pro-Asyl.
Een van de meest in het oog springende burgerinitiatieven is Grandhotel Cosmopolis in de Beierse stad Augsburg (Heber et al. 2011; Converso & Bron ND).[12] In een voormalig verzorgingshuis dat eigendom is van een protestantse kerk vestigden zich kunstenaars die naast eigen ateliers ook ruimte wilden geven aan vluchtelingen. Zij hebben een deel van het gebouw ingericht als studio's voor bewoning voor zichzelf en voor 65 asielzoekers – de deelstaatsoverheid wijst de appartementen toe aan asielzoekers als onderdeel van de vluchtelingenopvang. Een ander deel van het pand is in gebruik als hotel met zestien kamers. Vluchtelingen kunnen in dat hotel werken als onderdeel van hun voorbereiding op integratie in Duitsland (het zijn leer-werkplaatsen), onder andere in de keuken en in het café en de lobby. Daarnaast is er een podium waar optredens gegeven worden en dat open staat voor alle inwoners van de stad en er worden tentoonstellingen ingericht. Ten slotte worden er cursussen en consultancy-trajecten aangeboden op het terrein van (creatieve en interculturele) communicatie en veranderingsprocessen binnen organisaties.

Grandhotel Cosmopolis kan gezien worden als een *experimenteerruimte* te midden van een situatie die door velen opgevat wordt als bedreigend en onveilig. Deze nieuwe aanpak en vooral ook de alliantie tussen nieuwe actoren op het terrein van asielopvang lijkt vruchtbaar te zijn. Voorlopers als kunstenaars trachten via dit experiment het bewustzijn bij de Duitse bevolking te versterken dat de integratie van vluchtelingen hen niet alleen lasten hoeft te brengen, maar ook voordelen

[12] Zie: https://grandhotel-cosmopolis.org/de/

kan opleveren. De alliantie van deze kunstenaars met de protestantse kerk die het pand beschikbaar stelde en met de Lands-overheid die asielzoekers plaatst lijkt daarin cruciaal.

Op een aanverwante manier beschermen initiatieven van bedrijven om stages, werkervaringsplaatsen, en banen te creëren voor vluchtelingen twee waarden. De eerste is het economische belang van Duitsland om een grote speler in de wereld te blijven. Daarvoor zijn veel nieuwe arbeidskrachten nodig.
Het Duitse bedrijfsleven ziet vluchtelingen als een van de bronnen daarvoor. Tegelijkertijd voorkomt ook dit radicalisering omdat het inwoners oplevert die trots zijn deel uit te maken van een stad en een land. Op aandrang van het bedrijfsleven begonnen met name CDU-politici in 2018 een lobby voor een andere omgang met vluchtelingen met een baan. Eerder was al duidelijk geworden dat tamelijk veel vluchtelingen in Duitsland werk vinden. Onder de in 2015 aangekomen asielzoekers tussen 15 en 64 jaar heeft een kwart werk. De helft van hen heeft werk waarvoor een diploma nodig is (Deutschlandfunk, 2018). De SPD reageerde enthousiast op het CDU-initiatief, de CSU had wat bedenkingen. Op 2 oktober 2018 maakte de regerende Grote Coalitie bekend dat ze goed geïntegreerde, werkende uitgeprocedeerde immigranten een permanente verblijfsstatus zou gaan toekennen (Diekmann, 2018). Op deze manier is ook de *Wilkommenskultur* vanuit bedrijfsleven en burgerinitiatieven onderdeel van praktijken waarin op een heel andere, soms experimentele manier het hoofd wordt geboden aan dreigingen en waarmee waarden beschermd worden in Duitsland.

4.4 CONCLUSIES

De Duitse casus is op meerdere leerzaam in relatie tot onze zoektocht naar de contouren en kenmerken van de weerbare open samenleving. Het meest nadrukkelijke punt is wellicht dat de FDGO een vrij onomstreden richting wijzend kader biedt voor alle beleid. Bestuurders lijken zich mede daardoor te beseffen dat nadrukkelijke veiligheidsmaatregelen ten koste kunnen gaan van de openheid van de Duitse samenleving. Zij stappen niet al te lichtvaardig over de nadelen van maatregelen heen.

Uit de reacties van de Duitse overheid kwamen vooral stappen naar voren die even logisch als (te) laat ingezet lijken te zijn geweest. Het verzamelen van essentiële informatie door de belangrijkste overheidsorganen op het terrein van migratie en veiligheid en het onderling delen ervan had blijkbaar lang geen prioriteit gehad. Men heeft dat relatief slagvaardig ‘rechtgezet’ sinds 2015, maar de vertrouwensschade voor de overheid is enorm geweest. Indirect is dat misschien wel de grootste schadepost voor de openheid van de Duitse samenleving geweest. Het beeld van onvermogen en falen van de overheid voedde populisme en extremisme.
De aanscherping van het asielrecht en andere wetgeving was deels een antwoord op de grotere dreiging door onder meer de Gefährder, maar heeft ook populistische trekken. Dat geldt met name voor de verscherping van de politie- en detentiepraktijk. De openheid van de Duitse samenleving komt hiermee in meerdere opzichten onder druk te staan.

De *fact based* publieksgerichte beleidscommunicatie biedt weliswaar geen garantie voor het herwinnen van steun onder de bevolking, maar is in Westerse open samenlevingen toch een belangrijke basis voor het werven van vertrouwen. Alleen daarom al is het goed dat het in Duitsland nu intensiever gebeurt, ook rond het thema migratie en veiligheid. De grondigheid ervan kan hier en daar een voorbeeld zijn voor Nederland.

Dat geldt echter niet voor de symboliek van het Heimat-beleid, al is de feitelijke uitvoering ervan in Beieren (glasvezelnetwerken tot in alle 'uithoeken' van het land) geen onlogisch antwoord op het sentiment van sommige burgers door 'de' overheid niet gezien te worden. Het inspelen op het zo diffuse Heimat-thema brengt zoals hierboven vermeld desalniettemin politiek-maatschappelijk risico's met zich mee, ook voor de openheid van de samenleving. Daarbij komt dat het effect op veiligheid en veiligheidsgevoel twijfelachtig is.

5. Vertaalslag naar Nederlandse context: verstoringen rond de vluchtelingen kwestie

5.1 INTRODUCTIE

De Nederlandse situatie rond asiel en migratie lijkt in veel opzichten op de Duitse. Er worden vergelijkbare dreigingen gezien, deels vergelijkbare waarden en belangen geïdentificeerd, en ook vergelijkbare praktijken in het leven geroepen of versterkt. Toch zijn er ook belangrijke verschillen met de Duitse asiel- en migratieproblematiek. Wij zullen zowel de overeenkomsten als de verschillen hieronder weergeven, waarbij de nadruk ligt op wat Nederland zou kunnen leren van de Duitse situatie, en wat niet. Wij zullen ook hierbij de drieslag maken tussen geconstateerde dreigingen, waarden en belangen, en praktijken. Vooraf geven we kort een indruk van de historische context waarin de crisis van 2015/16 rond de vluchtelingenkwestie gezien moet worden.

5.2 DE NEDERLANDSE HISTORISCHE CONTEXT

Een belangrijk onderdeel van de context gaat terug naar de jaren negentig van de vorige eeuw toen door de Balkanoorlogen veel mensen zich gedwongen voelden te vluchten. Dit had sterk verhoogde aantallen asielverzoeken als gevolg, zowel in Nederland als in Duitsland. In 1992 zijn dat er in Duitsland 438.191 (Alink. 2006, p.143). Er ontstaan grote achterstanden in de behandelingen van de verzoeken en asielprocedures duren lang. Er is sprake van maatschappelijke onrusten van gewelddadige acties tegen buitenlanders. Politici spreken van een ‘crisis’ (Alink 2006, p.144).

Als reactie besluit Duitsland in 1993 om het recht op asiel uit de grondwet te halen, en ook door 'terugname-overeenkomsten te sluiten met landen als Bulgarije, Polen, Zwitserland en Tsjechië. Duitsland betaalt hen ook fors om hun grenscontroles te versterken (120 miljoen DM aan Polen, 60 miljoen aan Tsjechië) (zie voor een uitwerking Geuijen, 2004). Deze maatregelen kunnen gezien worden als voorlopers van de latere EU-deals met o.a. Turkije. Na het nemen van deze maatregelen lopen de aantallen asielzoekers in Duitsland terug.
De aantallen in Nederland lopen dan echter op. In 1993 werden in Nederland 35.399 asielaanvragen ingediend, waar in de drie daaraan voorafgaande jaren sprake was van circa 21.000 aanvragen. In 1994 zelfs 52.576.[13] Dat leidde ook in Nederland tot maatschappelijke en politieke onrust. In juli 1993 moeten asielzoekers overnachten in tenten in maisvelden. Staatssecretaris d'Ancona doet op televisie een dramatische oproep aan gemeenten om plaatsen beschikbaar te stellen: 'het ministerie springt van ijsschots naar ijsschots' (Geuijen 2004, p. 59). Deze discussie mondde eerst uit in een wijziging van de Vreemdelingenwet die vooral gericht was op het verkorten van asielprocedures. Een aantal jaren later kwam er een geheel nieuwe Vreemdelingenwet (VW 2000). Tijdens de voorbereiding van deze nieuwe wet in januari 1999, geeft de toenmalige staatssecretaris van Justitie (vreemdelingenzaken) Cohen aan dat deze wet noodzakelijk is vanwege een asielstelsel dat op ontploffen staat.[14] Vanaf 2001 dalen de aantallen asielverzoeken scherp. Vermoedelijk is een van de oorzaken daarvan het einde van de Balkanoorlogen. Een aantal jaren blijft het relatief rustig in de vluchtelingenkwestie.

Voor zowel Nederland als Duitsland is de EU-context van groot belang in de vluchtelingenkwestie. In een aantal Europese landen worden al vanaf het midden van de jaren tachtig vergelijkbare directe en indirecte maatregelen genomen om de aantallen asielverzoeken omlaag te brengen. Daaronder vallen bijvoorbeeld visumvereisten, en 'carrier sanctions': sancties die opgelegd worden aan vervoerders die mensen een land binnen brengen die geen recht hebben op verblijf. Vanaf de jaren negentig wordt door de lidstaten steeds sterker ingezet op het bouwen van een gemeenschappelijk asielsysteem in de Europese Unie: het Common European Asylum System (CEAS). Dat systeem is gericht op samen het hoofd bieden aan dit vraagstuk. De belangrijkste kenmerken ervan zijn dat dezelfde criteria worden gehanteerd voor het bepalen wie vluchteling is en wie niet, en dat de minimale omstandigheden voor asielzoekers overal ongeveer hetzelfde zijn. De bedoeling hiervan is om te voorkomen dat asielzoekers door zullen reizen van het ene naar het andere land omdat daar de omstandigheden en voorwaarden beter zijn.
Rond 2015 komen er opnieuw veel meer vluchtelingen naar Europa toe. Deze keer door de burgeroorlogen in Noord-Afrika en het Midden Oosten, vooral in Syrië. De vluchtelingen gaan vooral naar Duitsland en Zweden. In mindere mate ook naar Nederland (en andere Europese landen). In 2015 vragen 890.000 mensen asiel aan in Duitsland. In Nederland waren dat er in dat jaar 58.880.

[13] http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=37970ned&D1=0-13&D2=19&VW=T

[14] https://www.digibron.nl/search/detail/012ddc31e9730131d110a42c/cohen-asielbeleid-staat-op-ontploffen

Dat is iets meer dan het aantal asielaanvragen dat in 1994 in Nederland werd ingediend. In 2014 waren dat er ongeveer 24.000 en daarvoor lag het aantal rond de 14.000. In 2016 en 2017 daalden de aantallen naar iets boven de 31.000.[15]
Net als Duitsland lijkt ook Nederland in 2015 overvallen te worden door deze grotere aantallen.

Nederland voert een landgebonden asielbeleid ten aanzien van Syrische asielzoekers die in Nederland aankomen; bijna alle asielaanvragen worden ingewilligd op voorwaarde dat er geen contra-indicaties zijn.[16] In 2013 stond het aantal Syrische asielaanvragen in Nederland op de tweede plaats en bedroeg 19% van alle eerste asielaanvragen.[17]
Natuurlijk is het gemakkelijk om achteraf te constateren dat Europese landen, waaronder Nederland, mogelijk meer aandacht zouden kunnen hebben gehad voor zogenoemde 'early' of 'weak signals' en dat Nederland en ook Duitsland zich daarom overvallen voelden en niet helemaal voldoende voorbereid waren. Het kabinet constateert in de Integrale Migratieagenda dat in 2015 en 2016 gebleken is hoe belangrijk goede voorbereiding is om te voorkomen dat het vertrouwen in de overheid daalt, het draagvlak voor bescherming afkalft en polarisatie in de samenleving toeneemt. Uit deze constatering blijkt hoe belangrijk de historische context van de asielkwestie is, en ook dat Nederland wil leren van haar geschiedenis (Ministerie van Justitie en Veiligheid, 2018).

5.2.1 Dreigingsperceptie
Uit de analyse van het Duitse casus wordt duidelijk dat de dreigingen die daar tijdens de 'vluchtelingencrisis' van 2015/16 gezien worden enerzijds liggen in de koppeling van asiel met veiligheidsissues en anderzijds in de maatschappelijke polarisatie die gerelateerd is aan het bestaan van zeer verschillende en verschuivende perspectieven op asiel en vluchtelingen. In Nederland bestaan vergelijkbare dreigingspercepties, zoals onder andere blijkt uit documenten als de Kamerbrief 'Integrale migratieagenda' van maart 2018 (Ministerie van Justitie en Veiligheid, 2018), uit de analyses van het Analystennetwerk Nationale Veiligheid in het Nationale Veiligheidsprofiel (RIVM, 2016), en uit gesprekken die in het kader van dit rapport gevoerd zijn met experts.

Deze dreigingspercepties hebben ten eerste te maken met de aantallen migranten en vluchtelingen die op een niet door de overheid gereguleerde wijze bescherming komen vragen. In de Integrale Migratieagenda 2018 wordt benoemd dat de bestaande overheidsorganisaties hierdoor overbelast kunnen worden. Uit de Integrale Migratieagenda blijkt dat net als in Duitsland de vrees bestaat dat dit enerzijds kan leiden tot een beeld van de overheid die het probleem niet aankan.

---

[15] https://ind.nl/over-ind/cijfers-publicaties/paginas/asieltrends.aspx

[16] De IND neemt aan dat vreemdelingen uit Syrië die vanuit het buitenland terugkeren, bij of na inreis een reëel risico lopen op ernstige schade. Een vreemdeling uit Syrië komt in aanmerking voor een verblijfsvergunning asiel voor bepaalde tijd op grond van artikel 29, eerste lid, aanhef en onder b Vw als de vreemdeling geen actieve aanhanger is van het regime. Tenzij er sprake is van contra-indicaties, zoals gedragingen als bedoeld in artikel 1F of gevaar nationale veiligheid of verblijf in een derde veilige land.

[17] https://ind.nl/en/Documents/AT_December_2013.pdf

Anderzijds dat het kan leiden tot een beeld van vluchtelingen als 'veroorzakers van te grote lasten' voor ons, wat op zichzelf weer kan leiden tot maatschappelijke onrust en polarisatie in de samenleving (Ministerie van Justitie en Veiligheid, 2018, p.7) en daarmee uiteindelijk tot een aantasting van sociale en politieke stabiliteit en de nationale veiligheid (RIVM 2016, p.192).
Daarnaast worden er dreigingen gezien in de mogelijkheid dat mensen met jihadistische motieven via de asielprocedure het land binnen zouden kunnen komen. Zij verkrijgen daarmee toegang tot het grondgebied en zouden aanslagen kunnen plegen (RIVM 2016, p.145).
Een derde dreigingsperceptie die genoemd wordt is de kans op radicalisering, tijdens of na afloop van de asielprocedure. Een aantal experts benoemde de mogelijkheid dat de duur en onzekerheid tijdens de asielprocedure aanleiding zouden kunnen geven tot radicalisering. Ook werd benoemd dat de gebrekkige integratie van vluchtelingen en andere verblijfsgerechtigde asielmigranten op de arbeidsmarkt aanleiding zou kunnen geven tot radicalisering.

Een andersoortige dreiging is gerelateerd aan getraumatiseerde personen. Een respondent gaf aan dat het niet altijd duidelijk is of iemand verward is of jihadistische sympathieën heeft. Dit is een vraagstuk dat nadere aandacht behoeft.

5.2.2 Waarden en belangen
Als dreigingen geconstateerd worden op de bovengenoemde aspecten, wat wordt er dan bedreigd? Met andere woorden, wat zijn belangen die bedreigd worden en die als beschermwaardig worden gezien? Klassiek worden deze samengevat onder drie aspecten van nationaal belang (zie Geuijen, 2004).

Ten eerste gaat het om belangen die vallen onder onze *sociaal-culturele identiteit*. Dit kan worden opgevat als de acceptatie van en het vertrouwen in de bestaande instituties zoals de Rechtspraak, het openbaar bestuur en de wetenschap. Voor velen valt daaronder bijvoorbeeld ook de gelijkheid tussen verschillende categorieën mensen, zoals mannen en vrouwen en homoseksuelen. Ook de Nederlandse taal is voor velen onderdeel hiervan. Voor sommigen is de invulling daarvan ook de 'joods-christelijk-humanistische' identiteit.
Als de bescherming van de sociaal culturele identiteit als beschermwaardig wordt benoemd, dan wordt meestal daaraan gekoppeld dat het belangrijk is dat asielzoekers, vluchtelingen en andere migranten ook op dit aspect integreren in de Nederlandse samenleving, via taalverwerving, inburgeringstrajecten en werk. Dit zou ertoe leiden dat zij meer onderdeel worden van de samenleving en dat zou radicalisering tegen gaan.

Een tweede beschermwaardig belang dat wordt genoemd is het brede idee van (fysieke) *veiligheid.* Daaronder kan verstaan worden het voorkomen en bestrijden van (reguliere) criminaliteit. Meer recent wordt het ook wel ingevuld met het voorkomen en bestrijden van radicalisering en terrorisme. Vaak wordt radicalisering en terrorisme gekoppeld aan fundamentalistische opvattingen van de islam, veel minder vaak ook aan rechts-extremistisme en/of links- extremisme.

Een derde belang dat beschermd zou moeten worden is het nationale *economische belang*. Nederland moet niet te veel hoeven betalen voor de asielprocedure, maar ook voor het voorzien in huisvesting en dergelijke. In het verleden werd vaak ook verdringing op de arbeidsmarkt en op de huizenmarkt genoemd: migranten zouden banen en huizen weghalen van Nederlandse burgers.
Al deze aspecten van het economische belang lijken in de recente discussie minder prominent genoemd te worden dan een aantal jaren geleden. Nu ligt de nadruk relatief meer op identiteitskwesties (zie bijvoorbeeld het Zwarte Piet-debat). Mogelijk worden in de discussie rond asielzoekers en vluchtelingen economische belangen op dit moment als minder belangrijk gezien dan sociaal-culturele of veiligheidsaspecten. Het is echter ook mogelijk dat ze zo vanzelfsprekend zijn geworden dat ze niet meer genoemd worden, terwijl in de publieke discussies de andere twee aspecten wel vaak bediscussieerd worden. Zoals beschreven nemen in Duitsland de economische belangen een veel grotere positie in binnen de asieldiscussies, met name omdat het Duitse bedrijfsleven deze naar voren brengt.

Naast deze drie beschermwaardige nationale belangen is er ook een ander type beschermwaardig belang dat door sommigen genoemd wordt. Dat is de bescherming van de *mensenrechten van vluchtelingen*. Vooral ngo's als VluchtelingenWerk en Amnesty International benoemen dit belang, en ook de IND benadrukt dit aspect. In Duitsland wordt dit vooral genoemd door Pro Asyl. Zij benadrukken daarbij dat vluchtelingen vooral degenen zijn waarvan de veiligheid fundamenteel in het geding is geweest: zowel hun fysieke veiligheid (leven) als hun vrijheid. Deze ngo's menen daarom dat er meer aandacht zou moeten zijn voor het ondersteunen van vluchtelingen in het verwerken van trauma's die gerelateerd kunnen zijn aan de vlucht-oorzaken, maar die ook door de vlucht zelf zijn verergerd. Ook vinden deze ngo's dat vluchtelingen vooral ondersteund zouden moeten worden in het opbouwen van een leven in Nederland. Zij zien dat als noodzakelijk om het beschermwaardige belang van de mensenrechten van vluchtelingen inhoud te geven. Daarnaast zien ze het als een voorwaarde om te voorkomen dat mensen los blijven staan van de samenleving, waardoor de veronderstelde kans op radicalisering zou worden verkleind.

5.2.3. Veiligheidspraktijken
Welke praktijken zien we dan in Nederland om de benoemde bedreigingen van de beschermwaardige belangen te voorkomen en bestrijden?
a Nederland zet sterk in op het verduurzamen van *netwerksamenwerking. Verschillende respondenten* geven aan dat dit succesvol gebeurt:

- Verzamelen en delen van informatie door publieke organisaties, enerzijds over vluchtroutes en -aantallen, anderzijds over potentiële terroristen; deze samenwerking is ook internationaal versterkt, zowel tussen politiekorpsen als inlichtingendiensten;
- (Peer to peer) *training* met en tussen professionals op mogelijke aanwijzingen van radicalisering. IND, COA en DT&V maken gebruik van een speciaal voor deze organisaties ontwikkelde training van het Rijksopleidingsinstituut Radicalisering.

- Instellen van regionaal-bestuurlijk *overleg* dat verantwoordelijk wordt voor de plaatsing van asiel-opvanglocaties in plaats van het COA, waardoor het lokale (bestuurlijke) draagvlak toeneemt;
- Permanente verbinding tussen de migratieketen en de veiligheidsketen;
- *Taskforce* op rijksbreed hoog-ambtelijk niveau: bestaande uit alle directeuren en directeuren-generaal die met asiel- en migratie te maken hebben, tijdens de crisis in het leven geroepen en daarna in stand gebleven; deze zou nu ingezet kunnen worden om te kijken naar mogelijkheden om migranten perspectief te bieden op huisvesting, onderwijs en arbeid.
- *Flexibilisering* in het asielproces en de asielopvang. In de Integrale Migratieagenda wordt benoemd dat 'de verhoogde asielinstroom heeft laten zien hoe belangrijk het is om goed voorbereid te zijn op hun komst. Een gebrek aan voorbereiding kent immers een hoge prijs: het vertrouwen in de overheid daalt, draagvlak voor bescherming kalft af en polarisatie in de samenleving neemt toe.' (Ministerie van Justitie en Veiligheid, 2018, p.7). Daarom wordt besloten tot 'een flexibeler asielstelsel dat sneller en beter kan inspelen op ontwikkelingen in de instroom en maatschappelijk en financieel efficiënter is dan ad hoc maatregelen' (Ministerie van Justitie en Veiligheid, 2018, p. 7-8). Er worden buffers ingesteld bij COA en IND. Die waren er voor de huidige periode van hoge aantallen asielverzoeken nauwelijks. Dat heeft geleid tot situaties die vergelijkbaar zijn met die uit de de jaren negentig - zoals hierboven beschreven - toen staatsecretaris d'Ancona (in 1993) zei: 'het ministerie springt van ijsschots naar ijsschots' en staatsecretaris Cohen (in 1999) het had over 'een ontploffend asielsysteem'. In 2015 zagen we dat de wachtlijsten bij de IND opliepen en dat het COA in hoog tempo noodopvanglocaties – waaronder sporthallen en (leger)tenten – moest organiseren om te zorgen dat asielzoekers niet op straat zouden hoeven slapen. Dagelijks was in de media te zien en horen hoe asielzoekers elke paar dagen met bussen naar andere locaties vervoerd werden. Het dorp Oranje werd het symbool van deze acties, en van het verzet daartegen onder delen van de bevolking. Respondenten benoemen dat de buffer in de opvang is nu verhoogd is van 1250 bedden naar 5000, met daar bovenop 5000 binnen 6 weken, en nog extra op iets langere termijn. Ook voor de IND is het belangrijk om met een vorm van buffers te werken om te voorkomen dat professionals te snel ontslagen en aangenomen moeten worden. Vanwege de hoge kennisintensiviteit is er veel 'omsteltijd' nodig. Desondanks blijkt in oktober 2018 opnieuw dat de achterstanden bij de IND zijn opgelopen[18], en het COA ijlings zeer recent gesloten opvanglocaties wil heropenen.[19] De oorzaak daarvoor zou te vinden zijn in drie verschijnselen. Ten eerste een (lichte) verhoging van het aantal asielaanvragen, en ten tweede het al langer bestaande probleem dat vluchtelingen met een verblijfsvergunning in AZC's moeten blijven wonen omdat het lang duurt voordat zij huisvesting in gemeentes toegewezen krijgen.

[18] https://www.nrc.nl/nieuws/2018/09/10/wachttijden-voor-besluit-asielaanvraag-toegenomen-a1615941;
https://www.nrc.nl/nieuws/2018/11/02/vluchtelingenwerk-wachttijd-asiel-opgelopen-tot-ruim-veertig-weken-a2753696

[19] https://www.nrc.nl/nieuws/2018/10/18/coa-snel-5000-nieuwe-plekken-nodig-voor-asielzoekers-a2624998

- Zij bezetten daarmee plaatsen die eigenlijk bedoeld zijn voor asielzoekers tijdens de procedure. En ten slotte is het voor de IND lastig om snel goed personeel te vinden op een krappe arbeidsmarkt.

b Aanscherping van asielrecht en andere wetgeving en ook van bijbehorende praktijken.
Net als in Duitsland werden in Nederland het asielrecht en de bijbehorende praktijken verder aangescherpt. Meerdere respondenten vertellen dat er een steeds bredere check wordt gedaan van degenen die een asielaanvraag indienen. In Nederland is er een 100% screening, waarbij social media wordt gecheckt, ook kunnen telefoons worden uitgelezen tijdens het identificatie en registratieproces. Screening vindt ook plaats bij nareizigers. Dit betreft gezinsleden van asielstatushouders die zich bij de statushouders in Nederland mogen vestigen op grond van het nareisbeleid. In een van de interviews wordt aangegeven dat dit soort maatregelen inmiddels 'de nieuwe standaard [is] geworden'. Aangegeven wordt dat dit 'hoge politieke prioriteit' had, en dat deze praktijken mogelijk waren doordat asielzoekers onder het vreemdelingenrecht vallen. De vreemdelingenwet geef hiervoor een wettelijke basis. Daarbij werd nadrukkelijk vermeld dat dit soort praktijken altijd binnen de kaders van de wet vallen. Het bestuursrechtelijk kader geeft ruimere mogelijkheden tot dit soort praktijken dan het strafrecht. Een respondent geeft aan dat dit betekent dat zowel voor de wet als in de praktijk verdachten en criminelen op dit aspect meer rechtsbescherming hebben dan asielzoekers.

In verschillende interviews wordt verder aangeven dat professionals in de veiligheidsketen getraind worden om nauwlettend vreemde gedragingen en verdachte situaties in de gaten te houden. In een interview werd aangegeven dat er "geen enkele begrenzing" aan het veiligheidsstreven opgelegd werd door de politiek: "er wordt liever meer gecontroleerd dan strikt noodzakelijk om mogelijke dreigingen te voorkomen, dan dat de controles begrensd worden". Dat komt volgens de betreffende respondent door overwegingen rond draagvlak en door incidenten en feiten die naar buiten kwamen over aan IS gerelateerde terroristen. In meerdere interviews wordt echter benadrukt dat alle maatregelen en praktijken passen binnen de juridische kaders. In geen van de interviews wordt aangegeven dat de organisatie reflecteert op mogelijke aantasting van privacy of integriteit die plaats zou kunnen vinden.

c *Communicatie en transparantie* over aantallen en feiten: net als in Duitsland wordt bewust ingezet op communicatie naar publiek en media, tussen publieke organisaties, en met en naar de politiek. Een respondent vertelt dat er tijdens de periode van verhoogde aantallen asielverzoeken een 'asiel-*dashboard*' is opgezet waarop alle relevante cijfers werden vermeld, bijna geheel in pictogrammen. Dit werd gecommuniceerd met politiek, met relevante organisaties, en met het publiek. Een respondent gaf aan dat een resultaat daarvan was dat het vragen om openheid van zaken afnam. "Journalisten hadden er na enkele weken al geen belangstelling meer voor." Waar de transparantie onder andere bedoeld was om rust te brengen in het maatschappelijk debat hielp het geven van veel informatie dus niet heel veel. Een respondent constateert dat bleek dat de journalistiek toch vooral gefocust is op incidenten en minder geïnteresseerd in het publiceren van feiten.

d *Integratie- en participatie-beleid*
Net als in Duitsland starten activiteiten gericht op participatie deels al tijdens de asielprocedure, mede om radicalisering te voorkomen en te bestrijden. In Nederland gebeurt dit echter veel terughoudender dan in Duitsland. De opvang is een wachtperiode buiten de reguliere Nederlandse samenleving. Inmiddels is het COA-beleid aangepast en is er meer samenwerking met Sociale Zaken en Werkgelegenheid in het kader van integratie op arbeidsmarkt. Integratie van vluchtelingen is al lange tijd problematisch: hun situatie op de arbeidsmarkt is slechter dan die van andere migranten (zie o.a. Engbersen et al. (2015) en CBS (2016).
e *Internationaal beleid*
Een aantal respondenten benoemt dat een goed werkend Europees asielstelsel van het grootste belang is, ook voor Nederland. In het Nederlandse en in het EU-beleid zijn altijd al voornemens te vinden geweest over het voorkomen van (plotselinge en/of grote) aantallen asielzoekers en het reguleren van 'asielstromen'. Dat is ook terug te vinden in de Integrale Migratieagenda van maart 2018 (Ministerie van Justitie en Veiligheid, 2018). Daarbij wordt benoemd dat grondoorzaken (*'root causes'*) van vluchtelingen-genererende situaties moeten worden aangepakt (Ministerie van Justitie en Veiligheid, 2018, p.4). Daarnaast wordt benoemd dat opvang in de regio bevorderd moet worden. Dat moet mogelijk gemaakt worden via het investeren in transitlanden (zoals Jordanië, Libanon, en Turkije voor vluchtelingen uit Syrië) (Ministerie van Justitie en Veiligheid, 2018, p.6). Ook wordt benoemd dat er legitieme mogelijkheden moeten blijven om asiel te verkrijgen en dat er alternatieve migratiekanalen moeten worden ingesteld . En ten slotte wordt altijd aangegeven dat iedereen het ermee eens is dat alle landen gedeelde verantwoordelijkheid moeten nemen voor de opvang van vluchtelingen, binnen Europa via relocatie (vanuit o.a. Italië en Griekenland), en buiten Europa via hervestiging (via UNHCR, de vluchtelingenorganisatie van de VN) (Ministerie van Justitie en Veiligheid, 2018.
Iedereen heeft belang bij een goed werkende internationaal en Europees asielsysteem. In de praktijk blijken er echter grote problemen te bestaan om dit vorm te geven. Zo bestaan tussen de lidstaten van de Europese Unie grote waarden- en belangentegenstellingen die veroorzaken dat het komen tot een gezamenlijk beleid en praktijk verlamd raakt.
En het blijkt al vele jaren dat de bijdragen aan de budgetten van UNHCR stelselmatig te laag zijn om opvang in de regio menswaardig plaats te kunnen organiseren. Nederland draagt daar overigens meer aan bij dan vele andere landen. Ook zijn de beschikbaar gestelde relocatie- en hervestigingsplaatsen voor vluchtelingen al jaren veel te klein. Nederland stelde jarenlang 500 hervestigingsplaatsen beschikbaar, waaronder 250 voor Syriërs. In 2018 zijn dat er 1000, voor 2019 wordt dat aantal op 750 gesteld (Ministerie van Justitie en Veiligheid, 2018, p.11).

5.3 LESSEN UIT DE DUITSE CASUS

Er blijken veel overeenkomsten te zijn tussen Nederland en Duitsland, zowel in de historische als EU-context, in dreigingsperceptie, waarden en belangen, als ook in veiligheidspraktijken.
Op een aantal terreinen blijken beleid en praktijk in allebei de landen goed op orde. Zo is de (publieks)communicatie zowel in Nederland als in Duitsland een bewust speerpunt geworden.

Zoals ook bleek uit de analyse van de Duitse situatie, is dit geen garantie voor het herwinnen van steun onder de bevolking, maar is het wel een belangrijke basis voor het werven van vertrouwen.

Er zijn ook aspecten in beleid en praktijk die in Nederland beter zijn georganiseerd dan in Duitsland. Waar in Duitsland samenwerkingsproblemen (deels) voortkomen uit de situatie met de Länder, verloopt in Nederland de samenwerking steeds beter. Nederlandse experts geven aan dat het eerder zo is dat Duitsland qua netwerksamenwerking van Nederland kan leren, dan andersom.
Wat zijn de belangrijkste aangrijpingspunten voor Nederland om te leren uit de Duitse casus? Wij willen er twee benoemen. Het eerste gaat over de verhouding tot fundamentele principes, het tweede over nieuwe mogelijkheden voor weerbaarheid.

5.3.1. Pragmatisch handelen met reflectie op fundamentele principes
In Nederland lijkt het centrale uitgangspunt in veiligheidspraktijken wat meerdere respondenten benoemen als *'pragmatisch'* handelen. Voor hen betekent dit dat zij zo effectief en efficiënt mogelijk veiligheid trachten te bevorderen.
In de Duitse casus zien we dat er altijd een vanzelfsprekende reflectie is op het FDGO: de liberaal-democratische basisorde, die de bescherming van de open samenleving vooropstelt en de grondrechten van burgers. Tot de basisprincipes van het FDGO horen respect voor in de grondwet concreet beschreven mensenrechten, met name het persoonlijke recht op leven en vrije ontplooiing, volkssoevereiniteit, de scheiding der machten, de verantwoordelijkheid van de regering, de wetmatigheid van het bestuur, de rechterlijke onafhankelijkheid, het meerpartijenstelsel, en de gelijkheid van kansen voor alle partijen. Zoals de Duitse casus liet zien biedt deze FDGO een helder kader voor waar het bij de verdediging van democratie en rechtstaat concreet om gaat. Uit interviews en documenten blijkt dat Duitse politici en bestuurders doordrongen zijn van dit kader. In de opleiding van ambtenaren blijkt het FDGO steeds een expliciete rol te spelen, zoals blijkt uit een interview met de BKA. BAMF-vertegenwoordigers verklaren dat in de samenwerking met ngo's soms expliciet aan het FDGO wordt gerefereerd. Bestuurders lijken zich hierdoor goed van bewust dat nadrukkelijke veiligheidsmaatregelen ten koste kunnen gaan van de openheid van de Duitse samenleving. Zoals we eerder geconstateerd hebben, stappen zij niet lichtvaardig over de nadelen van maatregelen heen.

In de dagelijkse (overleg)praktijk in Duitsland wordt volgens diverse respondenten echter nauwelijks naar het FDGO verwezen. Mensen van het BKA benoemen het strafrecht en het strafprocesrecht als het kader voor hun dagelijkse functioneren. Daarbij vernamen wij van een Nederlandse respondent dat medewerkers van BAMF aangeven dat zij maar wat graag vergelijkbare screeningspraktijken zouden uitoefenen als in Nederland gebruikelijk zijn. Er lijkt dus ook in de dagelijkse veiligheidspraktijk in Duitsland sprake te zijn van een zekere mate van (behoefte aan) 'pragmatisch handelen' zoals dat in Nederland genoemd wordt.
Toch denken we dat Nederland zou kunnen leren van de vanzelfsprekendheid van reflectie op de fundamentele principes van de liberale democratie zoals dat in Duitsland meer gangbaar is.

Zo zouden bijvoorbeeld in de hedendaagse gangbare praktijken van screening explicieter fundamentele reflecties kunnen plaatsvinden over afwegingen rond de bescherming van privacy en persoonlijke integriteit.

5.3.2. Nieuwe mogelijkheden voor weerbaarheid via partnerschappen

In de Duitse casus zien we dat behalve veel overheidsorganisaties ook veel private partijen een belangrijke rol spelen in het vormgeven van de weerbare open samenleving. Weerbaarheid wordt daar niet alleen bevorderd door strakke veiligheidsmaatregelen, maar ook door de veerkracht van de samenleving te vergroten via meer inclusieve praktijken. Zoals we hierboven gezien hebben verwacht een aantal van de door ons gesproken Nederlandse en Duitse experts dat daarmee radicalisering van (voormalige) asielzoekers tegengegaan kan worden.

We hebben in de Duitse casus twee manieren gezien van *inclusieve praktijken* via partnerschappen. De ene wordt vooral gedragen door het Duitse bedrijfsleven. Zij focust op de economische kansen die migranten bieden, met name in het vullen van vacatures die structureel niet op andere manieren vervuld kunnen worden. Dit gaat in de Duitse casus zelfs zo ver dat in oktober 2018 bekend werd gemaakt dat goed geïntegreerde, werkende migranten een permanente verblijfsstatus zouden krijgen.[20] Het Duitse bedrijfsleven neemt daarmee de klassieke rol van het bedrijfsleven in kapitalistische systemen aan: het bevorderen van economische kracht via het aantrekken van meer beschikbare (goede en goedkope) arbeidskrachten. Dat resulteert er onder ander in dat in Duitsland meer vluchtelingen op de arbeidsmarkt zijn te vinden dan in Nederland.

In Nederland heeft het bedrijfsleven deze rol niet op zich genomen: het Nederlandse bedrijfsleven pleit, ondanks het groot aantal openstaande vacatures, niet openlijk voor meer immigratie. Natuurlijk werken Nederlandse bedrijven wel aan het openstellen van stages en arbeidsplaatsen voor migranten en vluchtelingen. Dat gebeurt ook al jaren in samenwerking met bijvoorbeeld het ministerie van Sociale Zaken en Werkgelegenheid. Daarnaast zijn er vele private initiatieven die vluchtelingen helpen integreren op de arbeidsmarkt: Refugee Start Force[21] en de Werkclub[22] zijn twee voorbeelden daarvan.

Een ander Duits voorbeeld van een partnerschap dat de veerkracht van de samenleving tracht te bevorderen is Grandhotel Cosmopolis[23] in Augsburg. Zoals we in de Duitse casus hebben beschreven werken hierin vluchtelingen samen met kunstenaars in leer-werkplaatsen in een hotel, café, en open podium. Er worden cursussen gegeven en consultancy trajecten aangeboden op het terrein van communicatie en veranderingsprocessen binnen organisaties. De protestantse kerk stelt het gebouw beschikbaar.

De deelstaatoverheid wijst de in het gebouw beschikbare appartementen toe aan asielzoekers als onderdeel van de vluchtelingenopvang. *experiment* versterkt het bewustzijn dat asielzoekers en vluchtelingen niet alleen een last hoeven zijn, maar ook voordelen kunnen opleveren voor de wijk

[20] https://www.nu.nl/buitenland/5492333/duitsland-zwakt-immigratieregels-af-wegens-arbeidstekort.html

[21] https://refugeestartforce.eu/

[222222] https://www.maatschappelijkealliantie.org/nieuws/de-werkclub-helpt-nieuwe-nederlanders-duurzaam-aan-het-werk

[23] https://grandhotel-cosmopolis.org/de/

en de stad. Vooral de nieuwe alliantie van partners lijkt hierin cruciaal: de overheid, de kerk, kunstenaars, de buurt, en de asielzoekers zelf.

Ook in Nederland zien we dergelijke innovatieve allianties tussen publieke en private actoren ontstaan. En ook hier bevorderen ze de weerbaarheid en veerkracht van de samenleving. Zo werd in Utrecht bijvoorbeeld 'Plan Einstein'[24] gestart waarin de gemeente Utrecht samen met traditionele ngo's als VluchtelingenWerk, en ook met nieuwe partners zoals de Social Impact Factory, de Volksuniversiteit en het Centre for Entrepreneurship van de Universiteit Utrecht samenwerkte. Bij het AZC aan de Einsteindreef in Utrecht werd woonruimte geschapen voor jongeren uit de wijk, als tegemoetkoming voor buurtbewoners die benoemden dat voor asielzoekers wel woonruimte beschikbaar kwam terwijl hun kinderen jaren moesten wachten op een woning. Er werden cursussen en ook individuele coaching aangeboden die gratis beschikbaar waren voor zowel asielzoekers, jongeren als buurtbewoners. En er werd een 'incubator space' ingericht waarvan iedereen uit de buurt en uit het AZC gebruik kon maken, om zich voor te bereiden op een cursus, om te werken, of om gewoon nieuwe mensen te ontmoeten. Waar Plan Einstein gefinancierd werd door de EU en de gemeente Utrecht, werden vele burgerinitiatieven opgepakt door vrijwilligers. Ook meldden zich vrijwilligers in grote getalen bij COA, VluchtelingenWerk. Zij geven aan dat ze op een bepaald moment net zoveel vrijwilligers hadden als vluchtelingen. Deze kracht vanuit burgers en organisaties kan gezien worden als een uiting van het weerbare karakter van de samenleving.

Een belangrijke tweede les uit de Duitse casus is dat in partnerschappen van overheidsactoren (waaronder de Arbeidsbureaus) en private actoren gekapitaliseerd wordt op de duidelijke *onderstroom van openheid* voor migranten en vluchtelingen. Het erkennen van en gebruiken van deze onderstroom draagt in potentie op de lange duur bij aan de oplossing van het migratie- en integratievraagstuk en is daardoor indirect van belang voor het versterken van de weerbaarheid van de open samenleving. De weerbare open samenleving heeft met andere woorden ook een duidelijke economische dimensie: is openheid (dan wel weerbaarheid) in economische zin profijtelijk?

5.4 BOUWSTENEN VLUCHTELINGENKWESTIE IN HET LICHT VAN DE WEERBARE OPEN SAMENLEVING

In dit hoofdstuk hebben we laten zien dat in Nederland al een aantal belangrijke bouwstenen voor veerkrachtig omgaan met verstoringen in de vluchtelingenkwestie aanwezig is.
Zo is er sprake van goed functionerende netwerken van cruciale organisaties. Er wordt veel informatie uitgewisseld, in toenemende mate ook internationaal en over sectoren heen.

[24] Formele naam is Utrecht Refugee Launch Pad U-RLP: https://www.uia-initiative.eu/en/uia-cities/utrecht

Ook is veel ingezet op (publieks)communicatie waarmee transparantie over keuzes en praktijken wordt bevorderd. Dit kan bijdragen aan het tegengaan van feitenloze debatten en het versterken van goed geïnformeerde discussies.

We hebben echter ook geconstateerd dat Nederland twee bouwstenen kan gebruiken uit de Duitse casus. De eerste is het explicieter reflecteren op fundamentele principes als mensenrechten, privacy, en persoonlijke integriteit in de (dagelijkse) veiligheidspraktijken. De Nederlandse prakijken zijn 'pragmatisch', in de zin van effectief en efficiënt. Het is belangrijk om naast het verder uitbouwen en versterken van deze instrumentele kant ook voortdurend expliciet te reflecteren op de principiële aspecten van het handelen als professional in organisaties. Daarmee wordt explicieter vormgegeven aan de balanceer act tussen weerbaarheid en openheid en is er meer oog voor de legitimiteit van de maatregelen.

De tweede bouwsteen gaat over de rol van publiek-private partnerschappen in het versterken van weerbaarheid en veerkracht van de samenleving. Ook dit is een aspect dat in de Nederlandse situatie al bestaat, maar dat verder versterkt kan worden. Dat vereist het creëren van ruimte en het faciliteren van burgerinitiatieven en initiatieven door het bedrijfsleven. De overheid hoeft daarin lang niet altijd een leidende rol te spelen. Soms is het weghalen van (wettelijke of financiële) barrieres en het coördineren van contacten tussen potentiële partners al een heel belangrijke stap.

Het combineren van bouwstenen die er in Nederland al langer zijn, met een aantal cruciale bouwstenen uit de Duitse casus kan bijdragen aan een goede balans tussen weerbaarheid en openheid bij verstoringen in vluchtelingenkwesties.

6. Cybersecurity in Israël

6.1 INLEIDING

In dit hoofdstuk wordt een exploratief onderzoek verricht naar de reactie op *cyber*dreigingen in Israël. Het hoofdstuk begint met een beknopte introductie op het thema *cybersecurity* en de rol die Israël speelt op dit terrein. Vervolgens wordt ingegaan op de Israëlische *cybersecurity*strategie en hoe hierin zowel bedreigingen als kansen een belangrijke rol spelen. Hierbij zullen ook de verschillende actoren binnen het vraagstuk *cybersecurity* in Israël aan de orde komen. Daarna volgt een beschrijving van de verschillende maatregelen en initiatieven die er vanuit de Israëlische overheid zijn genomen om de *cybersecurity* te vergroten en de *cybersecurity*industrie te versterken.

De Israëlische casus laat zien hoe de overheid in samenwerking met de private sector en universiteiten innovatie en economische groei op het gebied van *cybersecurity* kan stimuleren. Daarbij zal expliciet worden stilgestaan bij de politieke en sociale context van het *cyber*vraagstuk in Israël. Als het gaat om *cybersecurity* zijn niet-technische elementen, zoals de nationale cultuur en politieke belangen, doorslaggevend voor de richting van het overheidsbeleid en de maatregelen die worden genomen (Tabansky & Ben Israel, 2015, p.71). De specifieke nationale context waarbinnen deze ontwikkelingen plaatsvinden is daarom van groot belang om deze ontwikkeling te begrijpen.

6.2 CYBERSECURITY

De talloze digitale technologieën die inmiddels onderdeel zijn geworden van ons dagelijks leven hebben gezorgd voor vele nieuwe mogelijkheden. Ook de overheid maakt veelvuldig gebruik van digitale technologieën. Op het vliegveld kun je tegenwoordig via *'eGate'* zelf je paspoort scannen, de drukte op de snelweg wordt gemeten middels sensoren in het wegdek, en de overheid stapt over op e-facturen die handmatige verwerking van de facturering onnodig maken.

Tegelijkertijd maakt de toenemende afhankelijkheid van digitale technologieën onze samenleving kwetsbaar. Het gebruik van digitale systemen, netwerken en technologieën brengt het risico met zich mee dat deze door organisaties of individuen worden gehackt.

Aanvallen op de systemen van grote bedrijven kunnen grote economische gevolgen hebben en statelijke actoren weten zelfs door digitale beïnvloeding van verkiezingen nationale democratische processen te saboteren (NCTV, 2018). Het World Economic Forum heeft eerder in 2018 *cyber*dreiging aangemerkt als één van meest prominente mondiale risico's van deze tijd (World Economic Forum, 2018, p.6). De omvang van de digitale dreiging neemt bovendien toe (NCTV, 2018, p.5).

Het lastige van *cyber*dreigingen is dat ze van dag tot dag kunnen variëren. Dreigingen zijn namelijk sterk afhankelijk van technologische ontwikkelingen. Aangezien de ontwikkelingen op dit terrein zeer snel gaan kan er zich vrij plotseling een nieuwe dreiging voordoen. Hierop is moeilijk te anticiperen. Daarnaast ziet het vraagstuk *cybersecurity* op het aanpakken van uiteenlopende dreigingen; van *cyber*spionage door statelijke actoren, *cyber*sabotage van vitale sectoren, *cyber*criminaliteit voor financieel gewin tot *cyber*terrorisme (Munnichs et al., 2017). Dit maakt het lastig om een omvattende nationale *cyber*securitystrategie te ontwikkelen die oplossingen biedt voor de veelheid aan mogelijke *cyber*dreigingen die zich kunnen manifesteren.

Israël staat bekend als een van de wereldleiders als het gaat om *cybersecurity*. De aandacht voor technologische en wetenschappelijk innovatie op dit terrein is in Israël erg groot. De Israëlische *cybersecurity*industrie is een belangrijke speler op de internationale markt. Zo is in Israël het grootste aantal NASDAQ genoteerde bedrijven buiten Noord-Amerika gevestigd (Start-Up Nation Central, 2018). Diverse grote hightech multinationals, zoals IBM, Cisco Systems en Microsoft, hebben een kantoor in Israël (Start-Up Nation Central, 2018) Daarnaast zijn er de laatste jaren talloze *startups* opgericht die werken aan innovatieve producten en diensten op het gebied van *cybersecurity*. Inmiddels zijn er in Israël meer dan 300 bedrijven bezig met *cybersecurity*, een verdubbeling sinds 2012 (Start-Up National Central, 2018). Dit heeft Israël wereldwijd een plaats opgeleverd tussen de koplopers.

6.3 DREIGINGEN EN KANSEN

Interessant aan de Israëlische *cybersecurity*strategie is dat deze in feite stoelt op twee pijlers: nationale veiligheid en economische ontwikkeling. In eerste instantie speelde *cybersecurity* met name een rol in het kader van het nationale veiligheidsbeleid van Israël. De afgelopen twintig jaar is er echter ook nadrukkelijk aandacht geweest voor de mogelijkheden van *cybersecurity* voor de economische ontwikkeling van het land. Sindsdien heeft Israël zich ontwikkeld tot wereldwijde *cybersecurity* grootmacht. Hierna zullen beide pijlers van de *cybersecurity*strategie worden toegelicht.

6.3.1 Cybersecurity en nationale veiligheid

Binnen het nationale veiligheidsbeleid heeft *cybersecurity* in Israël altijd een belangrijke rol gespeeld. De grote belangstelling daarvoor in Israël hangt samen met de constante dreiging waar het land mee te maken heeft (Tabanksy & Ben Israel, 2015, p.71).

Tegen de achtergrond van de ingewikkelde geopolitieke context waarin Israël zich bevindt heeft zich een nationaal *security* concept ontwikkeld waarbij technologie en (digitale) informatieverzameling een belangrijke rol spelen. De sterke groei van de Israëlische *cybersecurity*industrie moet dan ook mede worden bezien in het licht van het conflict in het Midden-Oosten. De Israëlische respondenten die hiernaar zijn gevraagd beamen allemaal dat deze context zorgt voor een constant gevoel van urgentie als het gaat om veiligheid, wat een voedingsbodem biedt voor de ontwikkeling van nieuwe producten en diensten op het gebied van *cybersecurity.*

De eerste stappen op het gebied van *cybersecurity* werden in Israël in 2002 gezet op het terrein van het beschermen van de vitale infrastructuur tegen *cyber*aanvallen (Tabansky & Ben Israel, 2015, p.35). Voor *cybersecurity* in deze sector geldt een streng regime waarbij bedrijven en publieke organisaties die door de overheid zijn aangemerkt als onderdeel van de vitale infrastructuur – zoals rechtbanken, het gevangeniswezen, de Bank of Israel, energiebedrijven, havenbedrijven, Israel Railways en de aandelenbeurs – verplicht veiligheidsmaatregelen moeten nemen om hun digitale systemen te beschermen.[25] Er is bovendien een speciaal agentschap opgericht, NISA, dat verantwoordelijk was voor het vaststellen van de criteria waaraan het *cybersecurity*beleid van specifieke overheidsorganisaties en private bedrijven die verantwoordelijk zijn voor de vitale infrastructuur aan moeten voldoen (Housen-Couriel, 2017).

De Israëlische inlichtingen- en veiligheidsdiensten en het leger spelen een sleutelrol in het ontwikkelen en testen van innovatieve technologische oplossingen (Tabansky & Ben Israel, 2017, p.12). Inlichtingen spelen een cruciale rol in het Israëlische veiligheidsconcept. Zo heeft de Israëlische politie sinds 2012 een aparte *cyber*afdeling die zich bezighoudt met *cybercrime* en het centrale aanspreekpunt vormt voor kennis op het gebied van digitale forensische opsporing en digitaal bewijs (Housen-Couriel, 2017, p.13). Eén van de respondenten legde uit dat omdat de Israëliërs in aantallen vrijwel altijd in de minderheid zijn ten opzichte van hun vijanden, technologie een oplossing bood om toch successen te oogsten op veiligheidsgebied. Geavanceerde technologieën waarmee *real time* inlichtingen konden worden verzameld en verwerkt bleken met name instrumenteel in het preventief onschadelijk maken van zelfmoordaanslagen (Tabansky & Ben Israel, 2015, p.13).

6.3.2 De rol van het IDF

Een belangrijke rol in ontwikkelingen op het gebied van de *cybersecurity* is weggelegd voor het Israëlische leger (*Israel Defence Force*, IDF) (Rijksdienst voor Ondernemend Nederland, 2015, p.19).

---

[25] Resolution B/84 of the National Security Ministerial Committee of December 11, 2002 - *The Responsibility for Protecting Computerized Systems in de State of Israel*.

Het IDF maakt gebruik van *cyber*technologieën om de militaire capaciteiten van Israël te versterken (Tabansky & Ben Israel, 2015, pp.63-69). (Informatie) technologieën en de daaruit voortvloeiende militaire voordelen zijn essentieel voor het Israëlische veiligheidsbeleid.[26] De constante vraag naar IT-oplossingen om de militaire positie van het IDF te versterken vormt een sterke stimulans voor de ontwikkeling van technologische innovaties. Gelet op de gevoeligheid van veiligheidsoverwegingen in zijn algemeenheid worden details met betrekking tot *cybersecurity* binnen het leger nauwelijks gedeeld met het publiek.[27]

De sterke aandacht voor *cybersecurity* binnen het leger zorgt er echter wel voor dat een deel van de bevolking gedurende het vervullen van de dienstplicht kennismaakt met de nieuwste en meest geavanceerde *cyber*technologieën. Veruit de meerderheid van de Israëli's vervult vanaf zijn 17e levensjaar ten minste twee tot drie jaar dienstplicht. Bij binnenkomst worden de dienstplichtigen gekeurd en op basis van hun kwaliteiten ingedeeld bij een bepaalde unit. Dit kan ook bij één van de cyberunits van het IDF zijn. Dit betekent dat er binnen het leger jaarlijks een significante groep cyberexperts wordt opgeleid met *state of the art* kennis van *cyber* binnen een hightech omgeving (Rijkdienst voor Ondernemend Nederland, 2015). Bovendien speelt de dienstplicht een belangrijke factor in de veiligheids*mindset* van de Israëliërs. Volgens diverse respondenten worden jongeren in het leger getraind om alert te zijn op gevaar en ondernemend en resultaatgericht te werk te gaan. Deze hooggeschoolde *cyber*experts vormen na afloop van hun dienstperiode interessante arbeidskrachten voor het academische vakgebied en voor de vele technologiebedrijven in Israël. De *cybersecurity*industrie in Israël steunt dan voor een belangrijk deel ook op de kennis en ervaring die *cyber*experts tijdens hun militaire training bij één van de technologisch units van het leger hebben opgedaan (Tabansky & Ben Israel, 2015, p.19).

6.3.3 Israëlische cybersecuritystrategie

In 2010 werd *cybersecurity* een expliciete nationale doelstelling, toen minister-president Netanyahu het 'National Cyber Initiative' lanceerde (Housen-Couriel, 2017, p.8). Op verzoek van minister-president Netanyahu werd de Israëlische aanpak omtrent *cybersecurity* kritisch onder de loep genomen door een ad hoc multidisciplinaire commissie bestaande uit deskundigen uit het leger, ministeries, universiteiten en de private sector. Dit National Cyber Initiative had als taak om te komen met voorstellen voor maatregelen om Israël een leidende positie in de wereld te bezorgen op het terrein van *cybersecurity* (Housen-Couriel, 2017, p.8). Deze commissie ontwikkelde een meer omvattende *cybersecurity*strategie (Tabansky & Ben Israel, 2015, p.47). Het rapport van de commissie van deskundigen met een lijst met aanbevelingen werd in 2011 overgenomen door de Israëlische regering (Housen-Coureil, 2017, p.8). Eén van de aanbevelingen betrof de oprichting van een National Cyber Bureau (INCB), dat in 2012 werd opgericht (Housen-Couriel, 2017, p.8).

---

[26] En niet alleen voor verdedigingsdoeleinden. Buitenlandse bronnen wijzen er op dat Israël ook cybertechnologie ('cyberwapens') gebruikt om zelf aanvallen op zijn vijanden uit te voeren. Zie ook Tabansky & Ben Israel (2015), pp. 63-69.

[27] Informatie hierover hebben we daarom niet in het onderzoek betrokken. Zie ook Housen-Couriel (2017), p.9.

Het INCB was verantwoordelijk voor het coördineren van de ontwikkeling en uitvoering van de nationale strategie.[28]

Verschillende aanbevelingen in het kader van het National Cyber Initiative zijn vervolgens uitgewerkt in nadere regelgeving, in het bijzonder in Government resolutions nr. 2443[29] en nr. 2444.[30] Onderdeel van deze resolutions was de oprichting van een National Cyber Security Authority (NCSA). Naast het INCB heeft de NCSA een operationele rol in het versterken van de *cybersecurity* in de private sector.[31] In 2017 zijn de INCB en de NCSA samen ondergebracht in het Israeli National Cyber Directorate (INCD). Het directoraat is sindsdien de organisatie die verantwoordelijk is voor zowel de ontwikkeling als de uitvoering van de nationale *cybersecurity* strategie.

De *cybersecurity*strategie waar het INCD van uit gaat is gebaseerd op staatsinterventies die direct gericht zijn op de aanpak van *cyber*dreigingen enerzijds en indirecte inspanningen vanuit de overheid om *cybersecurity*activiteiten in de private sector te ondersteunen en te faciliteren anderzijds. Deze aanpak richt zich op drie lagen: Aggregate Cyber Robustness, Cyber Resilience van systemen, en National Cyber Defense (National Cyber Directorate, 2017, pp.9-13). Deze drie lagen hebben verschillende doelstellingen en de rol die de staat speelt in het realiseren daarvan varieert. Aggregate Cyber Robustness ziet op het vermogen van organisaties en processen om de meeste cyberdreigingen te voorkomen en af te slaan. Dit wordt gerealiseerd door *cybersecurity*inspanningen van organisaties en bedrijven te promoten (denk aan *best practices*, begeleiding, en het bieden van *incentives*). De Cyber Resilience van systemen ziet vervolgens op de aanpak van cyberaanvallen voor, tijdens en na het moment waarop ze plaatsvinden, door waar mogelijk te voorkomen dat ze zich verder verspreiden en hun schadelijke gevolgen te beperken. Hiervoor zijn informatieverzameling en -deling en het bieden van hulp aan organisaties en bedrijven tijdens een aanval van groot belang. Hierbij heeft het National Cyber Event Readiness Team (CERT-IL) een belangrijke taak. National Cyber Defense, tot slot, heeft betrekking op nationale defensieoperaties gericht op het aanpakken van cyberaanvallers. Deze pijler van de *cybersecurity* valt niet onder het INCD. In deze derde laag is een belangrijke rol weggelegd voor de nationale politie, de veiligheidsdiensten en het leger.

6.3.4 Cybersecurity: dreiging en economische kans

De Israëlische *cybersecurity*strategie zoals die in 2010 is ontwikkeld ziet niet alleen op het tegengaan van dreigingen, maar ook op de mogelijkheden voor strategische ontwikkelingen (Tabansky & Ben Israel, 2015, p.47). Israël beschikt over veel *human capital*: arbeidskrachten met ICT kennis en vaardigheden.

---

28 Resolution No. 3611 of the Government of August 7, 2011 - *Advancing National Cyberspace Capabilities*.

29 Resolution No. 2443 of the Government of February 15, 2015 - *Advancing National Regulation and Governmental Leadership in Cyber Security*.

30 Resolution No. 2444 of the Government of February 15, 2015 - *Advancing the National Preparedness for Cyber Security*.

31 Resolution No. 2444 of the Government of February 15, 2015 - *Advancing the National Preparedness for Cyber Security*.

Verschillende respondenten benadrukken dat dit gegeven is benut door de Israëlische staat om de IT-markt, en in het bijzonder de *cybersecurity*industrie, te stimuleren. Minister-president Netanyahu spreekt dan ook in 2011 zowel van 'cyber risks' voor de nationale veiligheid als van 'cyber hopes' voor economische kansen voor het land (Adamsky, 2017, p.124). Dit lijkt te hebben gewerkt. Israël is de afgelopen decennia uitgegroeid tot één van de belangrijkste wereldwijde spelers als het gaat om *cybersecurity*. De commerciële *cybertech*industrie is van groot belang voor de Israëlische economie. De geschatte totaalwaarde van de Israëlische ICT-sector was in 2014 ongeveer 30 miljoen Euro (Housen-Couriel, 2017, p.5). De Israëlische *cybersecurity*industrie profiteert van buitenlandse investeringen. Tussen 2014 en 2015 zijn de investeringen door buitenlandse bedrijven in de Israëlische *cybertech*industrie met 20% gestegen (Housen-Couriel, 2017, p.5). Israël huisvest vele wereldwijd toonaangevende technologiebedrijven die zich onder meer bezighouden met *cybersecurity*, waaronder Check Point, Oracle, en IBM. De afgelopen jaren is daar bovendien een groot aantal *cyber-start ups* bij gekomen. Deze aanpak waarbij naast het tegengaan van dreigingen ook economische ontwikkeling een belangrijke pijler vormt zien we terug in de maatregelen en initiatieven die sindsdien door de Israëlische overheid zijn genomen.

6.4 PRAKTIJKEN

Het belang van *cybersecurity* is in Israël al vroeg erkend. Reeds sinds de tweede helft van de jaren '90 is door de Israëlische overheid geïnvesteerd in nieuwe technologieën en in kennisontwikkeling op gebied van *cyberspace* en *cybersecurity* (Tabansky & Ben Israel, 2015, pp.32-34). Aan het begin van de 21st eeuw zijn vervolgens de eerste stappen gezet in het vormgeven van een nationale *cybersecurity* strategie (Tabanksy & Ben Israel, 2015, p.35). In de loop van tijd zijn enorme bedragen aan buitenlandse investeringen binnen gehaald en heeft de Israëlische *cybersecurity*industrie zich ontwikkeld tot een belangrijke nationale en internationaal speler. Recent zijn bovendien de eerste stappen gezet tot een overkoepelende nationale *cybersecurity*wet. Hierna zal een aantal interessante ontwikkelingen in de Israëlische aanpak van *cybersecurity* worden toegelicht.

6.4.1 Samenwerking tussen overheid, universiteiten en bedrijven

De *cybersecurity*strategie die in 2010 is ontwikkeld was gebaseerd op het idee dat de nationale *cybersecurity* gediend was met een sterke samenwerking tussen de overheid (inclusief het leger), universiteiten, en de industrie (Tabansky & Ben Israel, 2015, p.48). Eén van de belangrijkste constateringen bij het ontwikkelen van deze nationale strategie was dat hoewel *cyberspace* steeds complexer en meer verbonden was geworden, initiatieven met betrekking tot *cybersecurity* zich nog steeds beperkte tot overheidsnetwerken en de vitale infrastructuur. Informatie-uitwisseling met private netwerken buiten de overheid werd noodzakelijk geacht voor de effectiviteit van de nationale *cybersecurity*strategie (Tabansky & Ben Israel, 2015, p.55).

In de Israëlische strategie ligt de nadruk op samenwerking tussen wat wel de *'triple helix'* of het '*cybersecurity eco-system'* wordt genoemd: de overheid, technologiebedrijven en universiteiten.

Deze samenwerking wordt sterk door de overheid gestuurd door middel van verschillende incentives op het gebied van *cyber*bedrijvigheid. In de eerste plaats investeert de overheid in platforms waar dergelijke samenwerking kan plaatsvinden.

Voorbeeld: CyberSpark in Be'er Sheva
Een interessant voorbeeld hiervan is het CyberSpark Innovation Initiative in Be'er Sheva (CyberSpark, 2018). Dit initiatief werd in 2014 gelanceerd met de bedoeling om lokale technologiebedrijven, cybermultinationals, de overheid, het leger en universiteiten samen te brengen. Het project kwam tot stand door een samenwerking tussen het INCB dat onder de minister-president werkt, de gemeente Be'er Sheva, de Ben Gurion University of the Negev en een aantal grote technologiebedrijven die zich bezighouden met *cybersecurity*. Ook het IDF is bij het project betrokken (Housen-Couriel, 2017, p.14). In de woestijnstad Be'er Sheva is in 2013 een Cyber Innovation Arena opgericht, waar verschillende actoren binnen de triple helix zijn gevestigd (Rijksoverheid voor Ondernemend Nederland, 2015, p.20). Het CyberSpark Industry Initiative, een non-profit organisatie gevestigd in Be'er Sheva, is verantwoordelijk voor de coördinatie van de samenwerking tussen de verschillende actoren. Deze organisatie wordt gezien als een belangrijke speler binnen het Israëlische *cybersecurity* ecosysteem en biedt een platform voor het samenbrengen van de overheid, universiteiten, de *cybertech*industrie en het menselijk kapitaal op het gebied van *cybersecurity* (Housen-Couriel, 2017, p.14).

Sinds een paar jaar is in Be'er Sheva ook Israël's National Cyber Event Readiness Team (CERT-IL) gestationeerd. Deze dienst is het centrale nationale aanspreekpunt voor het omgaan met cyber security incidenten (met uitzondering van incidenten bij het leger en de vitale infrastructuur). De CERT-IL is in 2015 opgericht en maakte voorheen onderdeel uit van het NCSA (Housen-Couriel, 2017, p.13). Bedrijven en hun *cybersecurity* teams kunnen bij het CERT-IL terecht in het geval van *cybersecurity*-gerelateerde dreigingen en incidenten (Housen-Couriel, 2017, p.13). Het CERT-IL biedt een breed spectrum aan diensten die tot doel hebben om *cyber*dreigingen en de ernst daarvan in kaart te brengen, zoals een waarschuwingssysteem, technische assistentie in het geval van een cyberaanval en het geven van informatie om de digitale weerbaarheid te vergroten (Housen-Couriel, 2017, p.13). Daarbij maakt het CERT-IL gebruik van Cybernet, een systeem om informatie-uitwisseling op het gebied van *cybersecurity* te faciliteren. Het systeem maakt het mogelijk voor het CERT om verbinding te maken met de *cybersecurity* teams bij zowel publieke als private organisaties om informatie te delen over cyberaanvallen met als doel om nieuwe aanvallen te voorkomen (Housen-Couriel, 2017, p.13). Meer en meer bedrijven zijn aangesloten op dit systeem en delen *cybersecurity*-gerelateerde informatie met de overheid.

Uit interviews met verschillende respondenten blijkt dat deze samenwerking wordt vergemakkelijkt doordat de actoren binnen de 'triple helix' elkaar goed kennen. Het betreft een klein wereldje waarbij het netwerk dat jongeren tijdens hun militaire training opdoen van groot belang blijkt voor hun latere professionele contacten. Veel mensen die werkzaam zijn in de wereld van de *cybersecurity* in Israël kennen elkaar uit hun diensttijd waar ze vaak voor dezelfde *cyberunit* werkten. Meerdere respondenten geven aan dat dit het onderlinge vertrouwen versterkt.

Bovendien vindt er binnen de *cybertech*wereld veel roulatie plaats. De uniforme training van het IDF zorgt ervoor dat er gemakkelijk gerouleerd kan worden tussen verschillende posities. Veel Israëliërs die werkzaam zijn op het terrein van *cybersecurity* hebben dan ook bij de universiteit, én in het bedrijfsleven, én overheid een functie (gehad). Zo kan het goed zijn dat iemand die eerst jarenlang voor de overheid met *cybersecurity* bezig is geweest vervolgens een eigen *start up* opzet of bij een van de universitaire *cybersecurity* centra gaat werken en tevens als adviseur bij de overheid betrokken blijft. De verklaring die hiervoor wordt gegeven is dat er lange tijd sprake was van een tekort en nog steeds is aan *cybersecurity* professionals in Israël.

Uit de interviews blijkt ook dat een nadeel van de sterke nadruk op samenwerking is dat de verdeling van taken, rollen en verantwoordelijkheden tussen de verschillende actoren niet altijd duidelijk is. Onduidelijk is volgens verschillende respondenten wie er nu eigenlijk de leiding heeft in deze samenwerking.

6.4.2 Belastingvoordelen voor cybertechbedrijven in Be'er Sheva

Israël heeft wereldwijd de hoogste dichtheid aan *startups* per inwoner (Rijksoverheid voor Ondernemend Nederland, 2015). Ook op het gebied van *cybersecurity* kent Israël een groot aantal toonaangevende *startups*. Uit de gevoerde gesprekken blijkt dat het ministerie van Economische zaken via de Innovation Authority *cybersecurity startups* stimuleert door hen belastingvoordelen te bieden als zij zich vestigen in Be'er Sheva. Sinds een aantal jaren werkt de Israëlische overheid in Be'er Sheva samen met andere actoren die werkzaam zijn op het gebied van *cybersecurity* om van de woestijnstad in het zuiden van Israël een internationale 'cyber hub' te maken met internationale ambities. Cybertechnologiebedrijven worden door middel van onder andere kortingen op de loonheffing op het salaris van hun medewerkers aangespoord om zich binnen de Cyber Innovation Arena in Be'er Sheva te vestigen.[32]

6.4.3 Investeringen in wetenschappelijk onderzoek

In 2012 en 2013 is door de Israëlische overheid ongeveer 50 miljoen sjekel (ongeveer 11,8 miljoen euro) geïnvesteerd in wetenschappelijk onderzoek op het gebied van kunstmatige intelligentie en informatica (Tabansky & Ben Israel, 2015, p.52). Daarnaast zijn er dankzij het INCB sinds 2014 bij verschillende Israëlische universiteiten onderzoekscentra op het gebied van *cybersecurity* opgericht. Deze onderzoekscentra zijn deels gefinancierd door de overheid (Housen-Couriel, 2017, p.15). In het bijzonder de campus van Ben Gurion University of the Negev – gevestigd in het Cyberspark Cyber Innovation Arena in Be'er Sheva – is de laatste jaren uitgegroeid tot het cyberonderzoekscentrum van Israël. Het doel van de overheidsinvesteringen in deze universitaire *cyber research centers* is om innovatie op cybergebied te stimuleren door middel van wetenschappelijk onderzoek. Innovatieve cybertechnologieën die aan de universiteiten worden ontwikkeld kunnen volgens één van de respondenten via de vele startups vervolgens ten goede komen aan de vrije markt.

---

[32] Resolution No. 3611 of the Government of August 7, 2011 - *Advancing National Cyberspace Capabilities*.

6.4.4 Voorstel voor een nieuwe cybersecuritywet

In juni 2018 is door de Israëlische regering een wetsvoorstel ter consultatie voorgelegd voor een *Cyber Security and National Cyber Directorate Bill*.[33] Het wetsvoorstel heeft tot doel om het Israeli National Cyber Directorate (INCD) van een wettelijke grondslag te voorzien en tevens de bevoegdheden van dit directoraat uit te breiden (The Arab Center for the Advancement of Social Media, 2018). Het directoraat is hiërarchisch ondergebracht bij het bureau van de minister-president en is direct aan hem verantwoording schuldig (The Arab Center for the Advancement of Social Media, 2018). In het eerste jaar van zijn bestaan hield het directoraat zich vooral bezig met het sturen van het beleid op het gebied van *cybersecurity* in de private sector en de samenwerking met andere stakeholders. Het nieuwe wetsvoorstel beoogt het INCD een meer leidende rol te geven op het terrein van de nationale *cybersecurity*aanpak. De bedoeling van het wetsvoorstel is dat het directoraat verantwoordelijk wordt voor het inschatten van nationale *cyber*veiligheidsrisico's, het organiseren van de nationale *cyber*weerbaarheid en het adviseren van andere overheidsorganisaties en de private sector als het gaat om *cybersecurity*. Daarbij krijgt het INCD op grond van dit wetsvoorstel ook bevoegdheden op terreinen waarvoor andere toezichthoudende diensten verantwoordelijk zijn, zoals de financiële sector, de gezondheidssector en de transportsector (The Arab Center for the Advancement of Social Media, 2018).

Het wetsvoorstel voorziet in een vergaande uitbreiding van de bevoegdheden van het INCD op het gebied van *online* toezicht en dataverzameling bij zowel overheidsorganisaties als private bedrijven om een *cyberattack* te voorkomen of te bestrijden (Solomon, 2017). Het wetsvoorstel beoogt de medewerkers van het directoraat de bevoegdheid te geven al het internet verkeer in de gaten te houden en om computers en telefoons te *hacken* van ieder persoon, bedrijf of privéorganisatie die is aangemerkt als een gevaar voor de *cybersecurity*. De eerste 24 uur na het identificeren van een mogelijke dreiging mag het directoraat gegevens van deze apparaten verzamelen. Deze data zal worden opgeslagen in een nationale database met dreigingsfactoren (Council on Foreign Relations, 2018). Hoewel op grond van het wetsvoorstel voor de uitoefening van sommige bevoegdheden een voorafgaande rechterlijke beslissing is vereist, mag hier van worden afgeweken als volgens het hoofd van het INCD sprake is van bijzonderdere omstandigheden die direct ingrijpen vereisen (Cyber Security Research Center, 2018; Council on Foreign Relations, 2018). De medewerkers van het directoraat en bedrijven die medewerking verlenen aan het INCD zouden bovendien immuniteit genieten en kunnen niet aangeklaagd voor hun handelen (The Arab Center for the Advancement of Social Media, 2018).

Verschillende stakeholders zijn in principe positief over het feit dat er wetgeving komt op dit terrein. Ondanks de grote rol van *cyber*technologieën in het nationale veiligheidsdenken en het aanzienlijke aandeel van *cybersecurity* in de nationale economie, is er tot op heden nauwelijks wetgeving op dit terrein.

---

[33] Zie: http://www.tazkirim.gov.il/Tazkirim_Attachments/44319_x_AttachFile.docx. Helaas is er (nog) geen Engelse vertaling van het wetsvoorstel voor handen.

De Israëlische *cybersecurity*strategie[34] steunt op dit moment feitelijk op twee regelingen: Government resolutions nr. 2443[35] en nr. 2444.[36] Deze regelingen zijn een vorm van zogenaamde 'secondary legislation'. Dit is regelgeving waarbij de betrokkenheid van het parlement niet in alle gevallen is gegarandeerd.[37] De relatie tussen de staat en de private sector was op basis van deze regelingen vooral gebaseerd op vrijwillige medewerking door de markt. Met dit wetsvoorstel wordt echter een nieuwe koers ingezet. De *Cyber Security and National Cyber Directorate Bill* moet het INCD voorzien van het mandaat en de bevoegdheden om de greep van de overheid op de nationale *cybersecurity* te versterken.

Kritiek op het wetsvoorstel

Het wetsvoorstel roept in de Israëlische media echter ook veel weerstand op. Gelet op het grote marktaandeel van de *cybersecurity*industrie in Israël wordt regulering door velen gezien als een potentiële belemmering voor de economische groei van het land (Tabansky & Ben Israel, 2015, p.40). Daarnaast is één van de respondenten van mening dat wetgeving door zijn bureaucratische en trage karakter altijd achterloopt op technologische ontwikkelingen en daardoor ongeschikt is voor de regulering van *cybersecurity*.

Vervolgens zijn verschillende *privacy*verdedigers, burgerrechten-organisaties en *cybersecurity*specialisten van mening dat de bevoegdheden die in het wetsvoorstel aan de INCD worden toegekend veel te ver gaan en vrezen voor misbruik van deze bevoegdheden (Cyber Security Research Center, 2018; Council on Foreign Relations, 2018). Vanwege de verzameling en verwerking van grote hoeveelheden persoonlijke gegevens en bedrijfsgegevens die het wetsvoorstel beoogt, maken zij zich zorgen over de *privacy* van burgers en over de bescherming van bedrijfsgeheimen. Volgens sommige critici roept het wetsvoorstel het beeld op van het INCD als 'overheids-spionageapparaat' (Cyber Security Research Center, 2018).

Een eerste kritiekpunt ziet op de beperkte afbakening van de nieuwe bevoegdheden. Het wetsvoorstel schrijft namelijk niet voor hoe de data die worden verzameld mogen worden gebruikt en hoe lang de gegevens mogen worden bewaard (Calcalist, 2018). Mag deze informatie bijvoorbeeld gedeeld worden met de politie en ingezet worden tijdens een strafproces (Solomon, 2017)? Voorts wordt er kritiek geuit op de brede definitie van *cyber*dreiging en *cyber*aanval in het wetsvoorstel. Een *cyber*dreiging wordt volgens internetbronnen in het wetsvoorstel gedefinieerd als een poging *"to harm a democratic process"*.

---

34 Resolution No. 3611 of the Government of August 7, 2011 - *Advancing National Cyberspace Capabilities*.

35 Resolution No. 2443 of the Government of February 15, 2015 - *Advancing National Regulation and Governmental Leadership in Cyber Security*.

36 Resolution No. 2444 of the Government of February 15, 2015 - *Advancing the National Preparedness for Cyber Security*.

37 Basic Law: The Government (2001), art. 37 sub a. Alleen in geval van bepalingen die door straffen zullen worden gehandhaafd moeten deze regelingen *('regulations')* aan het parlement worden voorgelegd (Basic Law: The Knesset (1958), art. 21A (amendment 30). In het geval van deze *cybersecurity r*esolutions was goedkeuring door de Knesset inderdaad vereist.

Sommigen suggereren dat dit betekent dat de bevoegdheden van de INCD ook zouden mogen worden ingezet als een persoon of organisatie een bedreiging vormt voor de Israëlische economie. Ook vreedzame demonstraties tegen economische initiatieven zouden vervolgens onder deze definitie kunnen vallen (The Arab Center for the Advancement of Social Media, 2018). Een dergelijke brede definitie biedt ruimte voor misbruik van de gegeven bevoegdheden voor andere doelen dan die waarvoor ze zijn bedoeld (Calcalist, 2018).

Daarnaast wordt er in de wet gesproken van 'vitale belangen' die vergaande maatregelen zouden rechtvaardigen. Deze zijn echter zo breed gedefinieerd, dat ze dusdanig ruim kunnen worden geïnterpreteerd dat de bevoegdheden van de betrokken instanties nog verder worden opgerekt. Daar komt nog bij dat de wet een lijst met 'vitale belangen' bevat, die door de minister-president mag worden aangevuld (Cyber Security Research Center, 2018).

Een tweede kritiekpunt ziet op het feit dat het wetsvoorstel in onvoldoende *checks and balances* voorziet waardoor het INCD een te machtige positie zou krijgen (Calcalist, 2018). In veel gevallen waarin data worden verzameld, materiaal in beslag wordt genomen en gegevens worden opgeslagen komt er geen rechter aan te pas die voorafgaand de rechtmatigheid hiervan beoordeelt (Solomon, 2017). Gelet op de implicaties van de vergaande bevoegdheden van het INCD voor het recht op *privacy* wordt dit als zeer zorgwekkend ervaren (Solomon, 2017). Bovendien is het INCD direct verantwoording schuldig aan de minister-president, die tevens de autoriteit is die de prioriteiten stelt voor de strijd tegen *cyber*dreigingen (The Arab Center for the Advancement of Social Media, 2018).

Tot slot wordt gewezen op het gebrek aan transparantie van het werk van de INCD. Het wetsvoorstel schrijft niet voor dat de INCD het publiek op de hoogte moet brengen wanneer er een 'cyber hack' heeft plaatsgevonden. Geheimhouding is vaak cruciaal om een *hack* onschadelijk te maken. Achteraf zullen overheidsinstanties en bedrijven echter ook niet erg happig zijn om openbaar te maken dat ze zijn *gehackt* en dat er belangrijke data zijn buit gemaakt. De druk op het INCD zal dus groot zijn om deze informatie naar buiten te brengen, waardoor het publiek hier waarschijnlijk nooit weet van zal krijgen (Solomon, 2017).

Vooralsnog hebben we slechts te maken met een wetsvoorstel. Vanwege de controversiële nieuwe bevoegdheden die in het wetsvoorstel aan de INCD worden toegekend, is de verwachting dat het voorstel het wetgevingsproces niet zonder enige aanpassing zal doorlopen (Housen-Couriel, 2017). Dit is slechts een eerste stap in wat waarschijnlijk een lang en ingewikkeld wetgevingsproces zal worden. Het is daarom nog te vroeg om een uiteindelijk oordeel te geven over deze nieuwe *cybersecurity*wetgeving in Israël. Deze eerste plannen roepen echter nieuwe spanningen op in het licht van het beschermen van de bescherming van rechtsstatelijke waarden en fundamentele rechten in de weerbare open samenleving (Housen-Couriel, 2017).

6.4.5 Dataprotectie

*Cybersecurity*maatregelen hebben, zoals de discussie rond de *Cyber Security and National Cyber Directorate Bill* hierboven laat zien, vaak gevolgen voor de *privacy* van burgers en bedrijven. In een weerbare open samenleving moet een balans worden gevonden tussen het aanpakken van *cyber*dreigingen aan de ene kant en *privacy*overwegingen aan de andere kant. Dat dit ook voor Nederland een belangrijk thema is, bewijst de recente publieke discussie over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Deze wet voorziet in een uitbreiding van de bevoegdheden van de nationale inlichtingen- en veiligheidsdiensten, met name op het terrein van het verzamelen van gegevens van telefoon-, e-mail- en internetverkeer, om effectief te kunnen optreden tegen dreigingen zoals de voorbereiding van een terroristische aanslag of het hacken van belangrijke systemen (Kamerstukken II, 2016/2017). De grootste bezwaren tegen de nieuwe Wiv zagen op de gevolgen van de uitgebreide bevoegdheden voor de privacybescherming. Hieronder zal kort worden stilgestaan bij de *privacy*bescherming in Israël.

De Israëlische Grondwet die ziet op menselijke waardigheid en vrijheid is onder meer het recht op *privacy* gegarandeerd.[38] Artikel 7 sub a van deze Grondwet beschermt het recht van ieder persoon op privacy en intimiteit.[39] Dit recht is uitgewerkt in de Privacybeschermingswet, waarin bepalingen zijn opgenomen over de verzameling, gebruik en openbaarmaking van persoonlijke gegevens opgeslagen in digitale databases (The Privacy Protection Authority, 2017). In 2006 is door de minister van Justitie een Privacy Autoriteit opgericht.[40] Deze autoriteit houdt toezicht op de naleving van de wet- en regelgeving op het gebied van dataprotectie door privépersonen, bedrijven en de publieke sector.[41]

In mei 2018 is bovendien een aantal nieuwe regelingen met betrekking tot dataprotectie in werking getreden.[42] Deze aanpassing van het juridische kader is met name ingegeven door de

---

38 Israël heeft niet één Grondwet. Het constitutionele recht in Israël bestaat daarentegen uit een serie grondwetten die allen zien op een specifiek aspect van het Israëlische constitutionele recht. Zie voor de Grondwet die ziet op menselijke waardigheid en vrijheid uit 1992: https://www.knesset.gov.il/laws/special/eng/basic3_eng.htm.

39 Basic Law: Human Dignity and Liberty (1992), Art. 7. (a) (zie de onofficiële vertaling door dr. S. Hattis Rolef op de website van de Knesset: http://knesset.gov.il/laws/special/eng/BasicLawLiberty.pdf).

40 Israel Privacy Authority ("IPA", voorheen de Israeli Law, Information and Technology Authority), opgericht bij regeringsbesluit nr. 4660 (19.01.2006).

41 Art. 10 van de Privacybeschermingswet. Deze rapporten lijken niet in een Engelse vertaling voorhanden te zijn.

42 Privacy Protection (Data Security) Regulations (5777-2017 (PPDS)). Een Engelse vertaling van deze regelingen is helaas (nog) niet beschikbaar. Zie voor informatie over de inhoud van deze regels: https://www.gov.il/en/Departments/General/regulations_mechanisms. Deze regelingen ('regulations') zijn een vorm van secondary legislation, in dit geval afkomstig van de minister van Justitie. Goedkeuring door (een commissie van) de Knesset (het Israëlische parlement) is enkel vereist voor *regulations* die (deels) door middel van het strafrecht zullen worden gehandhaafd (Basic Law: The Knesset (1958), art. 21A (amendment 30)). In het geval van deze dataprotectieregelingen was goedkeuring door de Knesset inderdaad vereist. Deze goedkeuring is op 21 maart 2017 verleend. Er wordt echter wel gesuggereerd dat deze goedkeuring voor veel regulations slechts een "rubber stamp" is, zie http://knesset.gov.il/constitution/ConstP14_eng.htm.

Europese Algemene Verordening Gegevensbescherming (AVG) die sinds 25 mei 2018 van toepassing is en ook consequenties heeft voor de dataprotectie door Israëlische bedrijven, waarvoor de Europese Unie een belangrijke afzetmarkt vormt.[43] De nieuwe regelingen zijn van toepassing op zowel publieke als private partijen die persoonlijke gegevens verwerken. Afhankelijk van het type bedrijf of organisatie (hoeveel gegevens worden er opgeslagen, wat voor gegevens, en het doel van de gegevensverwerking) gelden er verschillende voorwaarden voor de gegevensverwerking (Ministery of Justice, 2017). Volgens de website van de Privacy autoriteit zijn deze regelingen tot stand na uitvoerige consultatie van de stakeholders op wie de regelgeving van toepassing is (The Privacy Protection Authority, 2017). Volgens één respondent worden juridische regels met betrekking tot databescherming echter door verschillende actoren ervaren als barrières voor een effectieve samenwerking en informatie-uitwisseling op het gebied van *cybersecurity*.

Als het gaat om privacybescherming is het van belang om niet alleen te kijken naar de waarborgen voor het recht op privacy in wet- en regelgeving, maar ook oog te hebben voor de status van privacy as culturele en sociale norm (Daskal, 2017). Tijdens verschillende interviews bleek dat privacy in Israël een andere status heeft dan in Nederland. Verschillende wetenschappelijke publicaties bevestigen dat in Israël socioculturele normen met betrekking tot privacy achterblijven op het juridische discours (Daskal, 2017; Karniel & Lavie-Dinur, 2012). Dit heeft deels te maken met de nadruk op het collectief in de Israëlische samenleving. De specifieke veiligheidscontext maakt ook dat privacy als belang slechts een marginale rol speelt in de samenleving. Onderzoek van het *Israel Democracy Institute* laat zien dat de meerderheid van de Israëlische burgers vergaande inperkingen van hun vrijheid accepteren met het idee dat ze daar meer veiligheid voor terugkrijgen (Daskal, 2017, pp.4-5; Hermann et al., 2016, pp.17-18). Dit beeld werd door verschillende respondenten in dit onderzoek bevestigd.

Desalniettemin heeft de Europese Commissie het privacybeschermingsbeleid van Israël adequaat bevonden in het licht van de AVG.[44] Dit betekent dat gegevensuitwisseling tussen EU-staten en Israël onder dezelfde voorwaarden plaatsvindt als tussen EU-staten onderling (European Commission, 2016). Wel is de verwachting dat de toegang van de overheid tot gegevens van burgers en bedrijven, zeker in het licht van de ontwikkelingen rond het voorstel voor een nieuwe cybersecuritywet zoals hierboven beschreven, de aandacht van Europa zal blijven trekken.[45]

---

[43] Art. 99 lid 2 EU Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PBLEU L 119/1 (4.5.2016).

[44] Besluit van de Commissie van 31 januari 2011 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, over de passende bescherming van persoonsgegevens door de staat Israël wat de geautomatiseerde verwerking van persoonsgegevens betreft (C(2011) 332), PBLEU L 27/39 (1.2.2011), p. 39–42. Zie ook art. 45 lid 1 van de AVG.

[45] De Europese Commissie houdt op basis van art. 45 lid 4 AVG doorlopend toezicht op ontwikkelingen in derde landen waarvoor een dergelijk 'adequate beschermingsbesluit' is genomen. Wanneer blijkt dat niet langer een passend beschermingsniveau in de zin wordt gewaarborgd kan de Commissie op ieder moment het besluit intrekken, wijzigen of schorsen (art. 45 lid 5 AVG).

6.5 CONCLUSIE

Cybersecurity is voor bedrijven, organisaties en nationale overheden een steeds belangrijker thema. In Israël staat het thema alle lange tijd op de agenda en het land staat bekend als wereldwijde koploper als het gaat om *cybersecurity*. Naast het feit dat de Israëlische overheid op grote schaal gebruik maakt van *state of the art* digitale technologieën om de nationale veiligheid te bewaken, heeft de *cybersecurity*industrie zich ontwikkeld tot een grote speler op de nationale en internationale markt. Het is daarom interessant om te kijken wat we in Nederland van deze Israëlische casus kunnen leren.

In de eerste plaats laten de ontwikkelingen in Israël zien dat de balans tussen *cybersecurity* aan de ene kant en het beschermen van de waarden van de weerbare open samenleving aan de andere kant niet gemakkelijk is. Zeker als het gaat om actuele en zware dreigingen is de roep om bevoegdheden voor de overheid om maatregelen te kunnen nemen om de veiligheid te kunnen garanderen groot. De Israëlische casus laat zien dat veiligheid als belang dominant kan zijn en dat in het kader van *cybersecurity* andere waarden van de weerbare open samenleving onder druk kunnen komen te staan. Dit wordt onder meer geïllustreerd door de heftige discussie over het wetsvoorstel voor een *cybersecurity*wet waarin de bevoegdheden voor het INCD in de strijd tegen *cyber*dreigingen worden uitgebreid, dat recent door de Israëlische regering gepubliceerd. Ook de beperkte aandacht voor dataprotectie in de Israëlische samenleving is hiervan een voorbeeld.

Ten tweede laat de Israëlische casus zien dat *cybersecurity* naast een reactie op dreigingen ook kansen biedt voor economische ontwikkeling. Israël heeft daar heel duidelijk de vruchten van geplukt. De sterke groei van de *cybersecurity*industrie in Israël, die het land binnen korte tijd tot een van de wereldleiders op dit terrein heeft gemaakt, is echter in belangrijke mate te danken aan de specifieke en unieke context van Israël. De continue dreiging voor de nationale veiligheid zorgt in Israël voor een constant gevoel van urgentie met betrekking tot veiligheid. Daarnaast zorgt de dienstplicht ervoor dat een deel van de bevolking in het leger kennismaakt met de nieuwste en meest geavanceerde *cyber*technologieën. Het resultaat is een *cybersecurity mindset* die gebaseerd is op veiligheid en innovatie en een vruchtbare voedingsbodem blijkt voor *cybertech*bedrijven en startups.

Tot slot laat de Israëlische casus zien dat samenwerking tussen de overheid, universiteiten en techbedrijven economische voordelen heeft. Het laat echter ook zien dat het bij die samenwerking belangrijk is dat er duidelijkheid bestaat over de verschillende rollen en verantwoordelijkheden van de verschillende actoren. Doordat in Israël de mensen die werkzaam zijn op het terrein van *cybersecurity* elkaar goed kennen en er veel roulatie plaatsvindt tussen posities, is de afbakening van taken en verantwoordelijkheden soms onduidelijk. Het is van belang dat de overheid waar nodig duidelijk een leiderschapsrol op zich neemt als het gaat om de naleving van wet- en regelgeving op het terrein van bescherming van de waarden van de open weerbare samenleving, waaronder privacybescherming.

7. Vertaalslag naar de Nederlandse context: Het cyber-security vraagstuk

7.1 INTRODUCTIE

De Israëlische situatie rond *cybersecurity* is vormgegeven door de sterke nadruk op veiligheid. Er worden in Israël vergelijkbare dreigingen geconstateerd rondom *cybersecurity* als in Nederland maar de gevoelde dreiging is van een heel andere orde dan die in de Nederlandse situatie. Dit heeft effect op de inzet op veiligheidspraktijken. In deze vertaalslag worden zowel de overeenkomsten als de verschillen beschreven. Hierbij ligt de nadruk ligt op wat Nederland kan leren van de Israëlische situatie en wat niet. Ook bij deze vertaalslag hanteren we de drieslag beschermwaardige waarden en belangen, de gepercipieerde dreigingen en de gehanteerde veiligheidspraktijken.

7.2 NEDERLANDSE CONTEXT RONDOM CYBERSECURITY

Nederland is een van de meest ICT-intensieve economieën ter wereld en daarmee een aantrekkelijk doelwit voor *cyber*criminelen, *cyber*spionnen en *hackers*. De aandacht voor het vraagstuk neemt toe, mede door diverse grootschalige *cyber*aanvallen die de afgelopen periode zijn uitgevoerd, de toenemende ongewenste buitenlandse inmenging in staten vanuit geopolitieke motieven, waarbij het doel is het verwerven van strategische informatie via spionage, en beïnvloeding van de publieke opinie of democratische processen. Of zelfs sabotage van vitale systemen, maar ook door alsmaar toenemende digitalisering van ons leven (*Internet of Things*) en daarmee de toegenomen kwetsbaarheid voor aanvallen en storingen. Het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Justitie en Veiligheid verklaart in het Cybersecuritybeeld Nederland (CSBN) van juni 2018 dat de omvang en ernst van de digitale dreiging in Nederland nog steeds aanzienlijk is en zich blijft ontwikkelen (NCTV, 2018).

Minister van J&V Grapperhaus geeft aan dat de aard en omvang van de dreigingen er niet om liegen en dat dit probleem daarom voor het kabinet een topprioriteit is (Ministerie van J&V, 2018 a). In navolging hierop trekt het kabinet eenmalig 30 miljoen euro extra uit voor *cybersecurity* (NOS, 2018). Dit plan vormt onderdeel van de begroting die op Prinsjesdag 2018 is gepubliceerd.

7.2.1 Beschermwaardige waarden en belangen

Het belang van goede *cybersecurity* in Nederland wordt door diverse partijen direct in verband gebracht met het borgen van de democratische rechtsstaat en waarden van onze open samenleving. Problemen op het gebied van *cybersecurity* worden door het RIVM (2016) gekoppeld aan dreigingen als 'Ondermijning', 'Financieel-economische bedreigingen' en de risicocategorie 'Cyberspionage'.

Volgens het Nationaal Veiligheidsprofiel zijn *cyber*spionage en *cybercrime* dreigingen die met een hoge waarschijnlijkheid zullen voorkomen in Nederland. Zij hebben weliswaar een vrij lage totale *impact* in termen van doden en gewonden maar kunnen wel specifieke nationale veiligheidsbelangen, zoals de sociale en politieke stabiliteit in het geval van ondermijningspraktijken door buitenlandse mogendheden, ernstig aantasten. Die specifieke belangen kunnen relevante aanknopingspunten zijn voor het versterken van de capaciteiten (RIVM, 2016).

Cybersecurity is daarmee direct te koppelen aan basiswaarden van onze weerbare open samenleving. Het gaat om de bescherming van de veiligheid van de systemen en de veiligheid van burgers, tegen diverse dreigingen zoals de toenemende inmenging van vreemde mogendheden in nationale verkiezingen van een land teneinde ons democratische systeem te beschermen. Dit betekent optreden om veiligheid te borgen aan de hand van de waarden van de democratische rechtsstaat. *Cybersecurity* is van belang om diverse vormen van veiligheid zoals beschreven in hoofdstuk 2 van dit rapport te borgen. Met name economische veiligheid en sociale/politieke stabiliteit vergen een gedegen *cybersecurity*systeem. Maar ook de fysieke veiligheid vraagt om *cybersecurity* om te voorkomen dat vitale infrastructuren door aanvallen van buitenaf worden aangetast.

Cybersecurity raakt dus direct aan de belangen van onze democratische samenleving en heeft een belangrijke rol in diverse economische en maatschappelijke belangen.

7.2.2 Dreigingsperceptie

Cybercrime is een 'veelkoppig monster'. In deze paragraaf gaan we kort in op het veelvormige karakter van de dreigingen op dit vlak zoals die in Nederland door verschillende betrokken organisaties worden gesignaleerd.

In Nederland is sprake van een continue digitale dreiging voor de nationale veiligheid aldus het CSBN 2018 (NCTV, 2018). *"De grootste dreiging vormen buitenlandse inlichtingendiensten die in ons land op grote schaal politieke, militaire en technologische informatie verzamelen en manipuleren.*

Cybercriminelen worden professioneler, de gebruikte methoden zijn geavanceerder en het verdienmodel winstgevender. Ook steeds meer mkb-bedrijven worden slachtoffer van cybercriminaliteit. De ontwikkeling van het Internet of Things versterkt die kwetsbaarheid. De beveiliging van "slimme" apparaten is vaak niet op orde waardoor ze kunnen worden gehackt en ingezet voor grootschalige DDoS-aanvallen. Cyberdreigingen ondergraven het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven en het vertrouwen in de digitale samenleving" aldus het persbericht van het Rathenau Instituut (2018) over een recent onderzoek over cyberdreigingen en versterking van de weerbaarheid (Munnichs et al. 2017).

Het NVP 2016 geeft een vergelijkbare analyse en schrijft het volgende over cyberdreigingen: *"Vanwege de groei van het digitale domein en de immer toenemende maatschappelijke afhankelijkheid van digitale systemen kunnen cyberdreigingen grote gevolgen hebben. Door de grote complexiteit van het digitale domein zijn cyberscenario's met grootschalige implicaties onzeker in aard, omvang en waarschijnlijkheid. Cyberincidenten kunnen zowel direct schade en ontwrichting veroorzaken (bijvoorbeeld door een omvangrijk datalek of de corruptie van belangrijke systemen) als indirect door verstoring van fysieke systemen. De impact van cyberincidenten ontstaat in een aantal gevallen niet zozeer door het incident zelf maar door uitval van vitale infrastructuur. Daarnaast kan de impact van (een serie van) cyberincidenten op zichzelf beperkt blijven, maar heeft de ondermijning van vertrouwen in digitale systemen uiteindelijk een grotere impact."* (RIVM, 2016, p 117).

7.2.3 Veiligheidspraktijken

Vanwege de bovenstaande bedreigingen doet de overheid een extra investering van 95 miljoen in *cybersecurity* en is een Nationale Cyber Security Agenda (NCSA) opgesteld. De NCSA is een kabinetsbrede agenda, waarmee volgens minister Grapperhaus een cruciale stap gezet wordt op weg naar een veiliger digitaal Nederland. De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen: [46]

1 Nederland heeft zijn digitale slagkracht op orde;
2 Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein;
3 Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software;
4 Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur;
5 Nederland werpt door middel van *cybersecurity* succesvol barrières op tegen cybercrime;
6 Nederland is toonaangevend op het gebied van *cybersecurity* kennisontwikkeling;
7 Nederland beschikt over een integrale, publiek-private aanpak van *cybersecurity*.

In het kort streeft Nederland hiermee naar een innovatiecultuur die doet denken aan de Israëlische innovatiecultuur. In Israël voert men dit echter nog verder door. Daar is men nog veel sterker gericht op innovatief denken en ruimte voor innovatie

[46] https://www.nctv.nl/binaries/CSAgenda_def_web_tcm31-322330.pdf

Er wordt dan ook gesproken van een echte start-up cultuur. Het veiligheidsdenken versterkt deze cultuur omdat er veel behoefte is aan nieuwe ontwikkelingen op dit vlak.

In het regeerakkoord van 2017 staat dat de extra middelen onder andere ingezet worden voor de uitbreiding van personele capaciteit en ICT-voorzieningen en verdeeld worden over de departementen Justitie en Veiligheid (NCTV), Defensie (MIVD), Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Milieu en Economische Zaken.

In de Nederlandse Cybersecurity Agenda (NCSA) zet het kabinet ook in op versterking van de samenwerking tussen betrokken partijen door inrichting van een landelijk dekkend stelsel van *cybersecurity* samenwerkingsverbanden. Door het opzetten van de Nederlandse *cybersecurity* alliantie verbinden publieke en private partijen zich om de maatregelen uit de NCSA verder vorm te geven (Ministerie J&V, 2018 b). Verder wordt onder meer ingezet op het versterken van het Nationaal Cyber Security Centrum (CCSC) als aanspreekpunt van 'Computer emergency response teams' (CERT) van alle sectoren, het stimuleren van *cybersecurity*onderzoek en het verbeteren van voorlichtingscampagnes op het gebied van *cyber*hygiëne.

7.3 LESSEN UIT DE ISRAËLISCHE CASUS

In deze paragraaf, die deels gebaseerd is op de masterscriptie van Berend Mutsaers (Mutsaers, 2018) (zie toelichting in hoofdstuk 3), staat de vraag centraal wat geleerd kan worden van de Israëlische casus voor de Nederlandse situatie in termen van haar veiligheidscultuur met betrekking tot *cybersecurity*. Daarbij zal in deze paragraaf de nadruk liggen op de vraag wat Nederland kan leren van de Israëlische veiligheidspraktijk rondom *cybersecurity*. Daartoe wordt eerst gereflecteerd op sterke punten van de Nederlandse veiligheidspraktijken en om te bezien op welke punten nog geleerd kan worden. Vervolgens wordt gekeken naar de overeenkomsten tussen beide casus. Daarbij gaat het met name om de gelijkenissen in de vraagstukken waarmee beide landen worstelen. Tenslotte wordt een overzicht gegeven van aspecten waarvan Nederland kan leren van de Israëlische veiligheidspraktijk rondom *cybersecurity*. Uiteraard dient hierbij rekening te worden gehouden met de specifieke nationale context in termen van weerbaarheid en openheid van Israël die op veel vlakken sterk verschilt van de Nederlandse. Daarom wordt bij de te leren lessen niet zozeer gedacht in termen van precieze praktijken maar meer over achterliggende principes die behulpzaam kunnen zijn bij het nadenken over en invulling geven aan de Nederlandse veiligheidspraktijken. Ook is er aandacht voor de implementatie van dergelijke praktijken door potentiële risico's te bespreken aan de hand van kritische kanttekeningen.

7.3.1 Overeenkomsten Nederland en Israël

In beide casuslanden wordt de koppeling gemaakt tussen de dreigingen én de economische kansen van *cyber*. Deze koppeling is in Israël echter al veel verder gerealiseerd dan in Nederland. Dit is inherent aan de context waarin het land verkeert.

Het land wordt gekenmerkt door een continu hoge dreigingsperceptie en heeft van deze ervaren nood, deels een deugd gemaakt door heel stevig te investeren in innovaties die ten dienste staan van haar veiligheid. Israël is te kenmerken als een echte innovatiecultuur en is mede daardoor wereldwijd een van de belangrijkste exporteurs van producten op het vlak van *cybersecurity*. In Nederland is de koppeling tussen maatschappelijke risico's en economische kansen veel minder ingegeven door gevoelde noodzaak maar vooral door een politieke ambitie. De *sense of urgency* is daarmee veel minder groot dan in Israël, terwijl de kaders waarbinnen deze bedrijven zich kunnen ontwikkelen, bijvoorbeeld op het gebied van privacywetgeving, veel strikter zijn. De ontwikkelingen gaan mede daardoor in Nederland minder snel. Ook wordt er door respondenten gesproken over de versnippering van kennis en expertise over verschillende centra in Nederland die zich op het gebied van *cybersecurity* profileren. Concentratie van deze kennis en expertise zou volgens hen de innovatiekracht ten goede komen.

Beide landen zien zich echter bij het werken aan het koppelen van de dreiging aan economische kansen geconfronteerd met vergelijkbare vraagstukken rondom de toekomst van *cybersecurity governance* en innovatie. Zo ervaren het Nederlandse NCSC als de Israelische tegenhanger INCD moeilijkheden met de aansturing van de private markt om te komen tot een goed beschermde markt. Beiden landen werken toe naar een minimaal te behalen niveau van *cybersecurity* over de volle breedte van de diverse ketens inclusief overheid, semioverheid en private partijen maar dit vraagt om een hele nieuwe verdeling en invulling van taken, verantwoordelijkheden en rollen tussen de marktsector en de overheid in het algemeen en de *cyber*-coördinator in het bijzonder.

Een tweede vraagstuk gaat over *data sharing*. Dit vraagstuk is zowel in Nederland als in Israël aangekaart. Omwille van juridische, institutionele en economische redenen is *data sharing* tussen verschillende partners binnen en tussen landen gelimiteerd. Volgens respondenten in beide landen vermindert dit het innovatieve vermogen van een land en daarmee de nationale weerbaarheid tegen cyberdreigingen.

Een laatste overeenkomst is dat beide landen een tekort hebben aan *cybersecurity* professionals. Voor de Israëlische casus klinkt deze constatering wellicht opmerkelijk – gezien de grote aanwas professionals die het IDF genereert. Niettemin blijft de vraag naar *cybersecurity* professionals in beide landen groter dan het aanbod.

7.3.2 Sterke punten Nederlandse context

Cybersecurity in Nederland wordt gekenmerkt door het bestuurlijke klimaat van het poldermodel en de focus op consensus tussen de vele en sterk verschillende partijen die in contact staan met elkaar. Zo wordt gewerkt aan unieke samenwerkingsprojecten zoals de Nationale Cybersecurity Research Agenda; een project waar Israël met grote interesse naar kijkt. Het ontbreken van hiërarchie in het Nederlandse model zorgt voor intensieve samenwerking in het *cyber*landschap.

Hoewel polderen ook gezien kan worden als een traag en log proces, zorgt de vanzelfsprekendheid van de constante interactie voor ruimte om kennis te delen en het creëren van nieuwe netwerken voor samenwerking. Dit is nog meer van belang gezien het tekort aan *cyber*professionals.

Het tweede aspect waarover respondenten spreken als een sterk punt op het gebied van *cybersecurity* haakt aan het vraagstuk van aansturing van de markt (zie paragraaf 7.2.1). Nederland zit namelijk in een ver gevorderd stadium met betrekking tot het bedienen van het Midden en Kleinbedrijf (MKB Nederland). De overheid heeft de ambitie om 1.6 miljoen middelkleine bedrijven te ondersteunen bij het veilig digitaal ondernemen (Rijksoverheid, 2018). Zij doet dit door het beschikbaar stellen van actuele informatie en betrouwbare adviezen en door het stimuleren van samenwerkingsverbanden van bedrijven die groepen ondernemers helpen met veilig digitaal ondernemen door middel van het beschikbaar stellen van subsidies (Rijksoverheid, 2018). Dit kunnen samenwerkingsverbanden in de keten, regio, sector of branche zijn. Deze bestuurlijke innovatieve manier van werken wordt eveneens met veel interesse vanuit Israël bezien.

Tot slot kent Nederland een sterke infrastructuur van organisaties en instituties die kennis hebben over of actief zijn op het gebied van *cyber*. Zo kennen wij onder meer de Amsterdam Internet Exchange (wereldwijd knooppunt voor internet), de internationale gerechtshoven in Den Haag (justitiële kant van cybercrime) en is er hoogwaardige kennis beschikbaar bij technische universiteiten in Nederland. Door zowel Nederlandse als Israëlische *cyber*professionals wordt de positie van Nederlandse universiteiten bezien als een van prominentste van de wereld. Dit sterke fundament kan gebruikt worden om de strategische economische ambities (zoals hierboven besproken) te realiseren.

7.3.3 Aangrijpingspunten voor Nederland

Hoewel de Israëlische context zoals gesteld sterk verschilt van de Nederlandse en er veel kanttekeningen te plaatsen zijn bij de wijze waarop Israël haar veiligheid borgt – zoals we verderop in dit hoofdstuk zullen doen –, kan Nederland daadwerkelijk op punten leren van de wijze waarop Israël haar veiligheidspraktijken op het vlak van *cybersecurity* heeft vormgegeven. Hieronder worden drie thema's besproken inclusief mogelijke concrete acties die daaraan gekoppeld kunnen worden.

Om te beginnen wordt de Israëlische samenleving gekenmerkt door een sterke *alertheid* op mogelijke dreigingen, zeker ook op het gebied van *cybercrime*. Dit bewustzijn is aanwezig in alle geledingen van de samenleving en leidt tot een breed gedeelde sense of urgency om te investeren in manieren om de dreigingen het hoofd te bieden waaronder *cybersecurity*.
Het bewustzijn wordt versterkt door de dienstplicht van drie jaar die Israël kent. In die periode doen Israëlische jongeren veel kennis op over mogelijke *cyber*dreigingen en wijzen om daarmee om te gaan. Maar de dienstplicht niet de enige *cyber*educatie die jongeren krijgen; al op jonge leeftijd worden ICT-kennis en vaardigheden aangeleerd.

Wat Nederland kan leren van de Israëlische situatie, is het principe van intensieve ICT *educatie en training* zoals dat in Israël richting jongeren wordt georganiseerd, niet alleen binnen het leger maar ook in het reguliere onderwijs. De Israëlische casus laat duidelijk zien dat de factor *human capital* essentieel is om op dit kennisintensieve domein te excelleren.

Het leger levert veel jonge mensen af met expertise op het vlak van *cybersecurity* die vervolgens een plek vinden binnen cyberkenniscentra. Omdat veel van de werknemers daar eenzelfde achtergrond kennen is er sprake van een hecht netwerk van vertrouwelingen. Dat maakt dat in Israël snel en eenvoudig gerouleerd wordt van plek door professionals tussen organisaties, zowel publiek als privaat. Deze typische Israëlische manier van werken zorgt niet alleen voor een kleine wereld (iedereen kent elkaar in cyber-land) maar ook voor een heel snelle en soepele uitwisseling van kennis en perspectieven.

In Israël is de *governancestructuur* rondom *cybersecurity* sterk gericht op kennisontwikkeling en innovatie en daarnaast op het creëren van een (export)markt voor *cyber*. De Israëlische overheid heeft veel geïnvesteerd in universitaire CyberCentres, innovatieve *cyber startups*, en belastingvoordelen voor *cyber*-bedrijven om zich in Be'er Sheva te vestigen. De overheid speelt daarmee een actieve rol in het stimuleren van het *cyber*ecosysteem. Deze *incentives* hebben geleid tot een flinke economische afzetmarkt voor cyber en miljarden aan buitenlandse investeringen. Kanttekening hierbij is echter dat de markt in Israël inmiddels zo groot is dat de overheid grip dreigt te verliezen. Volgens enkele respondenten bestaat zelfs het risico dat de markt de ontwikkelingen op het gebied van *cyber* in een richting stuurt die de kwaliteit van de innovaties niet ten goede komt. Het innovatieve vermogen kan daardoor in het gedrang komen en op termijn mogelijk zelfs de weerbaarheid tegen *cyber*aanvallen aantasten.

Daartegenover staan geluiden van respondenten die zich zorgen maken over de vergaande bevoegdheden die het recent door de Israëlische overheid ter consultatie voorgelegde wetsvoorstel wil toekennen aan het 'Israeli National Cyber Directorate' (INCD) en de beperkte bestuurlijke en rechterlijke controle die hierop mogelijk is. Dit kan ertoe leiden dat de Israëlische overheid veel meer bevoegdheden en data kan opeisen zonder dat er sprake is van een duidelijke controle daarop.

Beide scenario's laten zien dat het *cyber*veld gebaat is bij sturing en toezicht waarbij de beginselen van de democratische rechtsstaat leidend zijn. Zonder deze gebalanceerde sturing loopt een land het risico dat de krachten van de markt het speelveld gaan bepalen, danwel dat de overheid dermate centralistisch te werk gaat dat er geen sprake meer is van goede *checks and balances*. Beide scenario's kunnen tevens ten koste gaan van de innovatiekracht ten behoeve van het borgen van maatschappelijke weerbaarheid en stabiliteit.

7.4 BOUWSTENEN CYBERSECURITY IN HET LICHT VAN DE WEERBARE OPEN SAMENLEVING

Hierboven is een aantal aangrijpingspunten voor Nederland beschreven op het vlak van *cybersecurity.* De precieze vertaling naar de Nederlandse situatie is echter niet eenvoudig. Het is uiteraard niet wenselijk de maatregelen, die Israël neemt om de *cyber*dreigingen het hoofd te bieden, één-op-één te vertalen naar de Nederlandse situatie. De Israëlische veiligheidspraktijken dienen geplaatst te worden in het licht van de Israëlische veiligheidscultuur. Israël stuurt aan op een andere balans tussen weerbaarheid en openheid dan Nederland. Zo voert weerbaarheid in Israël veel meer de boventoon, ingegeven door een veel dominantere dreigingsperceptie.

De Israëlische casus laat zien dat de dreigingsperceptie grote invloed uitoefent op de veiligheidsstrategie in Israël. Binnen Israël bestaat een grote mate van bewustzijn van de dreigingen die gepaard kunnen gaan met het gebruik van digitale technologieën. *Cybersecurity* maakt onderdeel uit van het algemene veiligheidsdenken in Israël en staat (mede) daardoor hoog op de politieke en maatschappelijke agenda. De Israëlische samenleving kent daarmee veel meer dan de Nederlandse samenleving een aanhoudende *sense of urgency* om veiligheidspraktijken te ontwikkelen, aan te scherpen en daarvoor middelen vrij te maken. Dit biedt een stevige voedingsbodem voor technische ontwikkelingen op het gebied van *cybersecurity*.

Israël zet door de gevoelde continue dreiging, sterk in op bewustwording, weerbaarheid en praktijken om de veiligheid van digitale systemen en processen te borgen. Het leger, IDF, speelt hierbij een belangrijke rol. Maar er wordt door de Israëlische overheid ook buiten het leger veel geïnvesteerd in onderzoek en kennisontwikkeling op het gebied van *cybersecurity*, bijvoorbeeld bij een van de universitair *cybersecurity*onderzoekscentra die met financiële hulp van de overheid zijn opgericht. Naast weerbaarheid is ook economische ontwikkeling in Israël een dominant belang als het gaat om *cybersecurity*.

Belangen die gerelateerd zijn aan de open samenleving c.q. de democratische rechtsstaat zoals privacy en democratisch toezicht lijken ondergeschikt aan de weerbaarheid-gerelateerde en de economische belangen. Door de sterke nadruk op de ontwikkeling en toepassing van maatregelingen en technologieën om cyberdreigingen aan te pakken is er minder oog voor de mogelijke gevolgen voor privacy van de maatregelen die ingezet worden ten behoeve van het vergroten van de veiligheid. Het recent door de Israëlische overheid ter consultatie voorgelegde wetsvoorstel is hiervan een voorbeeld. Diverse juristen en mensenrechtenactivisten maken zich zorgen over de vergaande bevoegdheden die het wetsvoorstel aan het *Israeli National Cyber Directorate* (INCD) wil toekennen en de beperkte bestuurlijke en rechterlijke controle die hierop mogelijk is.

In Nederland is de balans tussen weerbaarheid en openheid delicater. Het optreden tegen *cyber*dreigingen staat hoog op de beleidsagenda maar de dreigingsperceptie speelt een minder dominante rol in de samenleving.

De discussie rondom veiligheidsmaatregelen gaat vaak over de balans tussen weerbaarheidsaspecten en aan openheid gerelateerde zaken zoals privacy en democratische controle, zoals bij de discussie en het referendum rondom de vernieuwde Wet op de inlichtingen en veiligheidsdiensten (Wiv) ook wel 'de sleepwet' genoemd.
Verder is in Nederland de scheidslijn tussen publieke en private organisaties en functies scherper dan in Israël. Roulatie tussen bijvoorbeeld publieke en private partijen en tussen verschillende sectoren is mede daardoor minder vanzelfsprekend. Bovendien roept het tegelijk vervullen van functies binnen het publieke en private domein in Nederland sneller vragen op omtrent belangenverstrengeling. Zo wordt verwezen naar het risico dat de combinatie van functies op publiek en privaat terrein gevolgen kan hebben voor de academische onafhankelijkheid die universitaire medewerkers genieten.

Kijkend naar de Israëlische veiligheidscultuur en de interactie tussen de dreigingsperceptie op het gebied van *cyber*, de veiligheidspraktijken en de beschermwaardige waarden en belangen in het bijzonder kan Nederland op de volgende punten lering trekken uit de Israëlische casus:

- Om te beginnen is de brede *bewustwording* van het gevaar dat uitgaat van cybergerelateerde dreigingen zoals die in Israël aanwezig lijkt, nog onvoldoende aanwezig in de Nederlandse samenleving. Uit een publieksconsultatie, uitgevoerd door SAMR in 2017 in opdracht van het ministerie van Buitenlandse Zaken in het kader van de Geïntegreerde Buitenland en Veiligheidsstrategie 2018-2022 onder ruim duizend Nederlanders, komt onder meer naar voren dat de respondenten zich t.a.v. internationale ontwikkelingen het meest zorgen maakt terrorisme (33%), internationale conflicten (30%) en deels over vluchtelingen (13%). Om cyberaanvallen is men amper tot niet bezorgd (0%) (percentages bij spontane benoeming dreigingen). De categorie cyberaanvallen krijgt bij geholpen beantwoording iets meer aandacht dan bij spontane beantwoording maar blijft alsnog hangen op een vrij magere 16%. [47]
- Ook is het principe van *flexibelere uitwisseling van kennis en ervaring* tussen verschillende organisaties, privaat en publiek en tussen verschillende sectoren, een leerpunt voor de Nederlandse situatie. Met name vanwege een tekort aan *cyber*professionals is de roep om zaken slimmer te organiseren nadrukkelijk aanwezig. Capaciteit blijft overigens ondanks deze makkelijkere kennisuitwisseling tussen en roulatie van personeel ook in Israël een probleem. Het blijven relatief kleine werelden met '*highly expertised*' personeel. Het investeren in en opleiden van nieuwe cyberexperts blijft een punt van aandacht.
- Verder laat Israël duidelijk zien dat *cybersecurity* naast een dreiging ook een kans kan zijn voor *economische* ontwikkeling. Israël plukt daar duidelijk de vruchten van geplukt. Dit punt is echter sterk gekoppeld aan de dreigingsperceptie die in Israël veel dominanter aanwezig is dan in Nederland.

---

[47] https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

- De kansen worden gecreëerd omdat men de noodzaak hoog acht en er derhalve veel middelen voor worden vrijgemaakt en ruimte geboden wordt in diverse opzichten aan nieuwe initiatieven die een bijdrage kunnen leveren aan de veiligheidspraktijken.
- De Israëlische casus laat tegelijkertijd zien dat veiligheid als belang dominant kan zijn en dat onder het mom van veiligheid en weerbaarheid rechtsstatelijke en democratische waarden onder druk kunnen komen te staan. De ontwikkeling van de *cybersecurity*industrie dient daarom hand in hand gaan met goed *toezicht* op de naleving van wet- en regelgeving op het terrein van fundamentele rechten (met name privacy). Er moeten waarborgen zijn dat er in het zichzelf versterkende proces van toenemende veiligheidsvergroting stevige *'checks and balances'* aanwezig zijn om de waarden van de democratische rechtsstaat te beschermen.

8. Conclusies en aanbevelingen

8.1 INTRODUCTIE

In dit hoofdstuk geven we zo goed als mogelijk antwoord op de hoofdvraag van dit rapport: *"Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?"*

Daaraan voorafgaand beantwoorden we de deelvragen zoals geformuleerd in hoofdstuk 1 van dit rapport. We starten daarbij met het beantwoorden van de deelvragen behorende bij de landencasuïstiek (8.2). Vervolgens geven we antwoord op de deelvragen betreffende de *lessons learned* vanuit de landencasuïstiek voor Nederland (8.3). In paragraaf 8.4 komen de overall reflecties en conclusies in termen van de WOS ter sprake, in het kader van de hoofdvraag die we in hoofdstuk 1 stelden. In paragraaf 8.5 sluiten we af met een reeks aanbevelingen/implicaties die van belang zijn om rekening mee te houden bij het dienen als bouwstenen voor de versterking van een weerbare open samenleving.

8.2 BEVINDINGEN CASUÏSTIEK

In de landencasuïstiek hebben we gezocht naar de antwoorden op de volgende deelvragen:

1 *Welke dreiging zien deskundigen in de betreffende landen rondom de gekozen thematiek voor de weerbare open samenleving? Welke waarden en belangen zijn daarbij beschermwaardig?*
2 *Welke praktijken worden gehanteerd om deze dreigingen het hoofd te bieden:*
   a *Welke mogelijkheden zien deskundigen in de betreffende landen om met technologische middelen of anderszins, disruptieve maatschappelijke ontwikkelingen in een vroegtijdig stadium te voorzien ?*
   b *Wat is de uitvoerbaarheid van deze maatregelen?*

c *Welke gevolgen hebben de snelle veranderingen van de dreigingen voor de (interne) organisatie van zowel private als publieke betrokken partijen en wat betekent dit voor de benodigde capaciteit?*[48]

d *In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?*

3 *Welke mogelijke gevolgen hebben de ingezette praktijken voor de weerbare open samenleving?*

Hieronder beantwoorden we deze deelvragen per casus.

8.2.1 Duitsland en het migratievraagstuk

1 *Welke dreiging zien deskundigen in Duitsland rondom asiel en migratie voor de weerbare open samenleving? Welke waarden en belangen zijn daarbij beschermwaardig?*
De dreigingen die in Duitsland gezien worden in het kader van het asiel en migratievraagstuk zijn uitgebreid besproken in hoofdstuk 4 van dit rapport. Wij zullen ons daarom hier beperken tot een meer algemene reflectie ten aanzien van de gepercipieerde dreigingen.
De vluchtelingencrisis is in Duitsland in zeer sterke mate een *legitimiteitscrisis* geworden voor het bestaande bestuurlijke bestel. Diverse ontwikkelingen zoals het chaotische opvangbeleid in de nazomer in herfst van 2015, het niet in staat zijn de grenzen te controleren, de vrouwvijandige incidenten in Keulen tijdens de jaarwisseling van 2015-16, de terroristische aanslagen in 2016 en het toenemend rechts-extremisme leidden tot verlies van vertrouwen in de gevestigde leiders en partijen en de overheidsorganen. Een en ander heeft tot gevolg dat Duitsland, ook volgens de respondenten gesproken in Duitsland, te maken krijgt met een groeiende polarisatie in de samenleving rond het thema asiel en migratie, een polarisatie die een aantasting betekent van de consensuele orde van de Bondsrepubliek en de maatschappelijke cohesie en het onderling vertrouwen van de burgers in elkaar ondermijnt.

2 *Welke praktijken worden gehanteerd om deze dreigingen het hoofd te bieden:*

a *Welke mogelijkheden zien deskundigen in de betreffende landen om met technologische middelen of anderszins, disruptieve maatschappelijke ontwikkelingen in een vroegtijdig stadium te voorzien?*
Met inachtneming van de onvoorspelbaarheid van sommige veiligheidsproblemen (met name van terrorisme) heeft de Duitse overheid hoge verwachtingen van de inrichting van nieuwe IT-systemen. Een belangrijk voorbeeld bleek de inrichting van de nieuwe omvattende IT-architectuur, Polizei 2020. De verwachting is steeds dat die technologische maatregelen het mogelijk maken zaken te verbeteren als het vroegtijdig signaleren en analytisch in kaart brengen van veiligheidsrisico's, het gerichter kunnen bestrijden van de betrokken organisaties en individuen; het coördineren van de verschillende politie- en veiligheidsdiensten en bijvoorbeeld de bij migratie betrokken diensten, en het (kunnen) informeren van politiek en publiek over de ontwikkelingen van criminaliteit (met als doel een genuanceerder en feitelijker debat).

---

48 De term "capaciteit" wordt breed opgevat. Het kan gaan over in te zetten mankracht, materieel maar ook over voldoende (beleids)maatregelen/instrumenten om een bepaalde dreiging aan te pakken.

Met andere woorden: de ontwikkeling sinds 2015 toont een sterker bewustzijn dat er geïnvesteerd moet worden in de IT-infrastructuur als voorwaarde voor boven genoemde overheidstaken, zodat de overheid veel slagvaardiger kan handelen in veiligheid gerelateerde uitdagingen als de vluchtelingen-crisis van 2015.
Er wordt sterk ingezet op dergelijke IT-maatregelen, zoals blijkt uit de centrale verzameling en analyse van gegevens over asielzoekers en andere migranten door de BKA en de informatievoorziening richting het publiek daarover.
Verder is ingezet op de sterkere betrokkenheid van niet primair op veiligheid gerichte overheidsdiensten zoals de migratiedienst BAMF bij die nieuwe centrale IT-systemen. Daarmee wordt ingezet op een grotere mate van bewustzijn binnen de brede overheid voor veiligheidsaspecten van het specifieke taakgebied. Zo stellen BAMF-medewerkers nu meer voor politie en veiligheidsdiensten relevante vragen in het eerste gehoor van asielzoekers en voeren deze antwoorden in een centraal IT-systeem in.

b *Wat is de uitvoerbaarheid van deze maatregelen?*
Er was en is in Duitsland sinds 2015 veel politieke en bestuurlijke wil aanwezig bij de verschillende diensten om zich gezamenlijk in te zetten voor de goede uitvoering van de voorgenomen maatregelen. Men ziet zich gezamenlijk voor de taak gesteld om het aangetaste vertrouwen in de overheid van grote delen van de bevolking en daarmee de legitimiteit van de overheid te herstellen. Het draagvlak binnen de betrokken diensten voor de ingezette maatregelen is daarom groot.
Tegelijkertijd wordt de politieke en bestuurlijk daadkracht danig op de proef gesteld door een partij als de AfD en andere populistische krachten, met name ter rechterzijde. Zij proberen garen te spinnen bij bestuurlijk falen. Hen is er veel aan gelegen het (beeld van) bestuurlijk onvermogen in leven te houden. Verder zien we dat sommige politici ter rechter- (CSU) en linkerzijde (de beweging #Aufstehen van Links-politica Sarah Wagenknecht) elementen van de populistische kritiek op het politieke stelsel overnemen en de legitimiteit ervan verder ondermijnen terwijl ze claimen de populisten de wind uit de zeilen te willen nemen.
Verder wijzen alle gesprekspartners op het Duitse federalisme als een factor die de, onder meer voor de IT-systemen, benodigde samenwerking altijd onder druk zet, omdat de deelstaten toch blijven hechten aan de eigen competenties.
De verbetering van de IT-systemen is erop gericht kennis over zogeheten Gefährder beter te kunnen verzamelen. Dit met het doel de kans op uitzetting van migranten die niet aan de voorwaarden voldoen voor het verkrijgen van een asielstatus te vergroten. In praktijk lukt het de verantwoordelijke diensten om praktische en bureaucratische redenen echter vaak niet een uitzetting daadwerkelijk te realiseren.

c *Welke gevolgen hebben de snelle veranderingen van de dreigingen voor de (interne) organisatie van zowel private als publieke betrokken partijen en wat betekent dit voor benodigde capaciteit?*
Voor 2015 is er in Duitsland jarenlang bezuinigd op met name de politie en de migratiedienst en de prijs daarvan werd duidelijk gevoeld. De grote toestroom van vluchtelingen stelde de betrokken diensten dan ook voor een groot capaciteitsprobleem in termen van mensen en middelen.

Sinds 2015 is er meer budget en meer personeel toegewezen aan de betrokken diensten om te kunnen omgaan met de veiligheidsaspecten gekoppeld aan de vluchtelingencrisis. De gesprekspartners begroeten deze trendbreuk, maar achten de benodigde middelen nog altijd ontoereikend. Een respondent verklaarde bijvoorbeeld dat de extra middelen vooralsnog vooral ingezet moeten worden om de schade van de eerdere bezuinigingen te repareren.

Wel worden de beschikbare capaciteiten beter geclusterd. Zo heeft het BKA een meer centrale rol gekregen in de verzameling en analyse van gegevens van nieuwkomers. Maar op het front van afstemming en samenwerking lijkt tegelijkertijd ook nog veel winst te behalen. Zo zijn de institutionele structuren van politie en veiligheidsdiensten nog maar beperkt veranderd sinds 2015. Dat geldt niet voor het BAMF. Enkele incidenten zorgden voor een reorganisatie van het bureau en uit hun organogram blijkt dat veiligheid een sterkere rol is gaan spelen na 2015 (meer secties houden zich daar deels mee bezig).

d In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?

Voor de beantwoording van deze vraag hebben we in de Duitse casus geen duidelijke aanknopingspunten kunnen vinden.

3 Welke mogelijke gevolgen hebben de ingezette praktijken voor de weerbare open samenleving?

Kijken we naar de balanceer act tussen veiligheid en openheid als het wezen van de weerbare open samenleving dan vergt dat een voortdurende reflectie op het optreden van betrokken overheidsdiensten. In Duitsland is dat in zekere zin door de tamelijk bewuste inkadering van het overheidsoptreden in de FDGO voorgeprogrammeerd. De FDGO biedt een nagenoeg *on*omstreden richtinggevend kader voor alle beleid. Bestuurders lijken er mede daardoor van doordrongen te zijn dat veiligheidsmaatregelen ten koste kunnen gaan van de openheid van de Duitse samenleving. Zij stappen niet lichtvaardig over de mogelijke nadelige effecten van veiligheidspraktijken voor de democratische rechtsstaat heen.

Het onder regie van het BKA verzamelen van essentiële informatie door de belangrijkste overheidsorganen op het terrein van migratie en veiligheid en het onderling delen ervan (dat blijkbaar lang geen prioriteit had gehad) heeft een goed *platform* gecreëerd voor 1) de signalering en 2) de bestrijding van migratie-gerelateerde criminaliteit en 3) de communicatie daarover met politiek en publiek. De verbeterde informatiepositie en de intensievere communicatie zijn echter relatief laat op gang gekomen. Bovendien is hier nog winst te behalen. De respondenten uit de Duitse casus uiten dan ook de wens dat er (nog) beter gecommuniceerd wordt met de burgers. Dit vanuit de constatering dat de legitimiteit van de overheid op dit vlak is aangetast en dus hersteld dient te worden. Het draagvlak dat wankel is geworden, moet worden onderhouden.

Wil een overheid zijn legitimiteit op dit terrein kunnen vasthouden of herwinnen, dan is een stevige *informatiepositie* wel een essentiële voorwaarde. De ‘fact-based’ publieksgerichte beleidscommunicatie is in westerse open samenlevingen bovendien een belangrijke basis voor het werven van vertrouwen.

Alleen daarom al is het goed dat het in Duitsland nu intensiever gebeurt, ook rond het thema migratie en veiligheid. De grondigheid ervan kan hier en daar zelfs een voorbeeld zijn voor Nederland.

Er is in Duitsland een duidelijke onderstroom van openheid voor migranten die tot uitdrukking komt in vele burgerinitiatieven, zoals het Augsburgse Grandhotel Cosmopolis, en in vele initiatieven en stellingnames uit het bedrijfsleven. Er zijn vele leertrajecten en vacatures voor asielzoekers en andere migranten geopend en in het Duitse asieltraject is ook een vaste rol voor het arbeidsbureau weggelegd. Relatief veel asielzoekers, ook uit de stroom van 2015, hebben inmiddels werk gevonden. Deze onderstroom draagt in potentie op de lange duur veel bij aan de oplossing van het migratie- en integratievraagstuk en is daardoor indirect van belang voor het versterken van de weerbaarheid van de open samenleving. Ze is ook een mogelijke bron van inspiratie voor Nederland.

Tegelijkertijd heeft de aanscherping van het asielrecht en andere wetgeving, deels in antwoord op de grotere gepercipieerde dreiging door onder meer de Gefährder, ook populistische trekken, met name de verscherping van de politie- en detentiepraktijk. De openheid van de Duitse samenleving komt hiermee onder druk te staan. Het Heimat-beleid mag op zichzelf geen onlogisch antwoord lijken op het sentiment van bezorgde burgers door ‘de’ overheid gezien te worden, maar het brengt voor de open samenleving wel risico’s met zich. Het Heimat-thema is bijvoorbeeld zo diffuus dat het allerlei oncontroleerbare verwachtingen met zich mee kan brengen. In potentie kan het de tweedeling en polarisatie daarmee versterken, terwijl het effect op veiligheid en het veiligheidsgevoel twijfelachtig is.

8.2.2 Israël en het cybervraagstuk

1 *Welke dreiging zien deskundigen in de betreffende landen rondom de gekozen thematiek voor de weerbare open samenleving? Welke waarden en belangen zijn daarbij beschermwaardig?*
De dreigingen die Israël signaleert in relatie tot het cybervraagstuk zijn uitvoerig beschreven in hoofdstuk 6 van dit rapport. Wij zullen ons daarom hier beperken tot een beknopte weergave van de gepercipieerde dreigingen. De bedreigingen van de *cybersecurity* (*cybercrime*, *cyber*terrorisme, *cyber*spionage) worden sterk gelinkt aan de algemene veiligheid van Israël. De dreigingsperceptie is een dominante en constante factor in de veiligheidscultuur van Israel. De samenleving is vooral gericht op mogelijke fysieke, geopolitieke of digitale aanvallen. Deze dominante dreigingsperceptie is de katalysator voor een sterke gerichtheid op (het investeren in) weerbaarheid. Daarnaast staan de economische belangen op het vlak van *cybersecurity* hoog op de agenda. Dit is eveneens te bezien als een vorm van weerbaarheid maar dan in economische zin.
2 *Welke praktijken worden gehanteerd om deze dreigingen het hoofd te bieden:*
    a *Welke mogelijkheden zien deskundigen in de betreffende landen om met technologische middelen of anderszins, disruptieve maatschappelijke ontwikkelingen in een vroegtijdig stadium te voorzien?*

Israel zet in op digitale weerbaarheid op verschillende niveaus. Deze digitale weerbaarheid is in ieder geval gericht op de vitale infrastructuren, maar ook steeds meer overheidsinstellingen en bedrijven die hun weerbaarheid op orde moeten hebben. De overheid heeft hierbij een sterk sturende rol. Het leger speelt een belangrijke rol in ontwikkeling van kennis en producten en in het sterk veiligheidsdenken in Israël. Daar komen *signaleren* en *innoveren* bij elkaar. Een belangrijk element voor vroegtijdig signaleren is volgens de Israëlische respondenten een breed bewustzijn van de mogelijke gevaren. Daar is in Israel veel aandacht voor zowel via het leger als via het reguliere onderwijs.

Ook wordt er veel geinvesteerd door de overheid in innovatiekracht via start ups en Cybercenters en vindt er veel kennisuitwisseling plaats tussen de diverse organisaties zowel publiek als privaat in termen van zowel samenwerking als roulatie van personeel. De gezamenlijke basis en gedeelde ervaring die de diensttijd biedt, versoepelt dat proces.

b *Wat is de uitvoerbaarheid van deze maatregelen?*
Weerbaarheid vereist nauwe samenwerking en intensieve kennisuitwisseling met het bedrijfsleven maar de relatie overheid/bedrijfsleven is delicaat. Het bedrijfsleven aan de ene kant wil graag profiteren van het gunstige investeringsklimaat in Israel maar heeft vaak geen belang bij het delen van informatie over *cybersecurity* en *cyber*aanvallen. De Israelische overheid wil graag bedrijven aantrekken vanuit economisch perspectief en vanuit het perspectief van innovatiekracht ten behoeve van de weerbaarheid. Tevens wil de overheid stevig grip hebben op het bedrijfsleven om die medewerking af te dwingen en een voor hen gewenste richting te sturen. Het voornemen van de overheid om zich via het nieuwe wetsvoorstel meer bevoegdheden toe te eigenen en toe te werken naar een centralistische vorm van sturing leidt tot weerstand zowel vanuit het bedrijfsleven als vanuit diverse (mensenrechten)organisaties (zie ook hoofdstuk 6).

c *Welke gevolgen hebben de snelle veranderingen van de dreigingen voor de (interne) organisatie van zowel private als publieke betrokken partijen en wat betekent dit voor de benodigde capaciteit[49]?*
We hebben geen precies beeld kunnen krijgen van de gevolgen van de toenemende *cyber*dreiging voor de capaciteit van betrokken partijen. Wel wordt breed aangegeven dat er ook in Israel (nog) sprake is van een tekort aan goede cyberexperts. De sterke samenwerking triple helix (overheid, universiteiten, bedrijfsleven) met sterk onderling vertrouwen en makkelijke uitwisseling van kennis en expertise biedt hier slechts ten dele een oplossing voor. Het blijft namelijk een kleine wereld met steeds dezelfde mensen. De behoefte bestaat daarom aan het vergroten van deze 'pool'.

d *In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?*
Er is geen specifiek zicht verkregen op welke specifieke onderdelen publieke organisaties ten aanzien van *cybersecurity* kunnen leren van de private ondernemingen.

---

49 De term "capaciteit" wordt breed opgevat. Het kan gaan over in te zetten mankracht, materieel maar ook over voldoende (beleids)maatregelen/instrumenten om een bepaalde dreiging aan te pakken.

Wel is duidelijk dat het bedrijfsleven sterk gericht is op innovatie en dat de Israëlische start up cultuur een grote innovatiekracht met zich meebrengt. Waar wellicht vooral van te leren is, is de mate van bereidheid van de overheid om te investeren in de onderzoekscentra zoals CyberSpark waar veel verschillende partijen samenkomen en elkaar versterken. Het belang van het faciliteren van samenwerking en innovatie is wat hier vooral uit spreekt.

3 *Welke mogelijke gevolgen hebben de ingezette praktijken voor de weerbare open samenleving?*
De dominante dreigingsperceptie is de katalysator voor een sterke gerichtheid op (het investeren in) weerbaarheid. Het leidt ook tot de sterke neiging tot centralistisch gestuurde controle door de overheid, zoals naar voren komt in het nieuwe wetvoorstel waarmee men vergaande bevoegdheden wil toekennen aan het *Israeli National Cyber Directorate* (INCD).

De dominante gerichtheid op weerbaarheid maakt tegelijkertijd dat er minder ruimte en aandacht is voor de andere zijde van de medaille. De sterke gerichtheid op *cybersecurity* maatregelen maakt dat andere belangen in het gedrang komen. Zaken als privacy, burgerrechten, rechtsstatelijke en democratische checks en balances staan duidelijk minder hoog op de agenda zoals wederom blijkt uit het nieuwe wetsvoorstel. Dit heeft mogelijke gevolgen voor het waarborgen van de privacy van burgers, voor bedrijfsbelangen, voor de balans tussen effectief optreden en rechterlijke en parlementaire controle, en voor interbestuurlijk toezicht. Kortom: de Israelische veiligheidscultuur wordt gedomineerd door de sterke dreigingsperceptie die maakt dat vooral ingezet wordt op veiligheidspraktijken om de weerbaarheid te verhogen. Belangen die meer gekoppeld kunnen worden aan de open samenleving staan daarmee minder hoog op de agenda.

8.3 GELEERDE LESSEN VANUIT DE DUITSE EN ISRAËLISCHE CASUS VOOR NEDERLAND

In hoofdstuk 1 zijn de onderstaande deelvragen geformuleerd die betrekking hebben op de lessen die Nederland kan trekken uit de hand van de landencasuïstiek.

1 *Wat kan Nederland leren van de betreffende landenpraktijken voor de inzet van maatregelen voor de weerbare open samenleving?*
2 *Wat kunnen de snel veranderende problematieken/dreigingen rondom onder meer asiel- en migratieproblematiek en cybersecurity betekenen voor (afstemming tussen) werkprocessen van Nederlandse (overheids)organisaties die verantwoordelijk zijn voor het Nederlandse veiligheidsbeleid onder meer als het gaat om agendering en besluitvorming en welke capaciteiten, zowel kwantitatief als kwalitatief (competenties) zijn nodig om de weerbaarheid van de Nederlandse overheidsorganisaties te versterken?*

In Nederland is een aantal belangrijke bouwstenen voor veerkrachtig omgaan met verstoringen in migratiekwesties al goed aanwezig. Zo is er sprake van goed functionerende netwerken van cruciale organisaties. Er wordt veel informatie uitgewisseld, in toenemende mate lukt dat ook internationaal en over sectoren heen.

Ook is veel ingezet op (publieks)communicatie waarmee transparantie over beleidskeuzes en veiligheidspraktijken wordt bevorderd. Dit kan bijdragen aan het tegengaan van 'feitenvrije' c.q. 'feitenloze' debatten die aanleiding kunnen geven tot polarisatie en tot ongefundeerde zorg die het draagvlak kunnen aantasten. Een solide feitenbasis is de voorwaarde voor goed geïnformeerde opbouwende discussies en voor vertrouwen in instituties.

We hebben geconstateerd dat Nederland twee bouwstenen kan gebruiken uit de Duitse casus voor het verder versterken van de weerbaarheid en openheid op het terrein van omgaan met migratiekwesties. De eerste is het explicieter in de (dagelijkse) veiligheidspraktijken reflecteren op *fundamentele principes* als mensenrechten, privacy en persoonlijke integriteit. De Nederlandse prakijken zijn 'pragmatisch', in de zin van daadkrachtig, effectief en efficiënt. Het is belangrijk om naast het verder uitbouwen en versterken van deze *instrumentele* kant ook voortdurend bewust te reflecteren op de *principiële* aspecten van het handelen als professionals in organisaties. Daarmee wordt uiteindelijk ook de weerbaarheid en openheid van de liberale rechtstaat versterkt.

De tweede bouwsteen gaat over de rol van *publiek-private partnerschappen* in het versterken van weerbaarheid en veerkracht van de samenleving. Ook dit is een aspect dat in de Nederlandse situatie al bestaat, maar dat kan verder versterkt worden. Dat vereist het creëren van ruimte voor en het faciliteren van burgerinitiatieven alsmede inititatieven door het bedrijfsleven. De overheid hoeft daarin lang niet altijd een leidende rol te spelen. Soms is het weghalen van (wettelijke of financiële) barrieres of het coördineren van contacten en belangenafwegingen tussen potentiële partners al een heel belangrijke stap. Dat kan ook leiden tot economische kansen.

Het combineren van de bouwstenen die in Nederland al langer bestaan met aanvullende cruciale bouwstenen uit de Duitse casus kan bijdragen aan een goede balans tussen weerbaarheid en openheid bij verstoringen in migratiekwesties.

Waar migranten soms als een dreiging in zichzelf worden gezien in het maatschappelijke debat is de brede *bewustwording* van het gevaar dat uitgaat van cybergerelateerde dreigingen zoals die in Israël aanwezig lijkt, nog onvoldoende aanwezig in de Nederlandse samenleving. Ook is het principe van *flexibelere uitwisseling van kennis en ervaring* tussen verschillende organisaties, privaat en publiek en tussen verschillende sectoren, een leerpunt voor de Nederlandse situatie. Met name vanwege een tekort aan *cyber*professionals is de roep om zaken slimmer te organiseren nadrukkelijk aanwezig. Verder laat Israël duidelijk zien dat *cybersecurity* naast een dreiging ook een kans kan zijn voor economische ontwikkeling. De Israëlische casus laat tegelijkertijd zien dat veiligheid als belang (erg) dominant kan zijn en dat onder het mom van veiligheid en weerbaarheid rechtsstatelijke en democratische waarden onder druk kunnen komen te staan. De ontwikkeling van de *cybersecurity*industrie dient daarom hand in hand gaan met goed *toezicht* op de naleving van wet- en regelgeving op het terrein van fundamentele rechten (met name privacy). Er moeten waarborgen zijn dat er in het zichzelf versterkende proces van toenemende veiligheidsvergroting tevens stevige *'checks and balances'* aanwezig zijn om de waarden van de democratische rechtsstaat te beschermen.

8.4 CONCLUSIES IN TERMEN VAN DE WEERBARE OPEN SAMENLEVING (WOS)

De hoofdvraag die wij in dit onderzoek hanteren, luidt:

- *Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?*

Op grond van de landenstudies, en de vertaling naar Nederland, kunnen we de volgende conclusies trekken aangaande het omgaan met de spanning tussen weerbaarheid en openheid.

Voor alles geldt dat de *dreigingsperceptie* van groot belang is voor de beslissingen rondom de inzet van veiligheidsmaatregelen. De dreigingsperceptie vertoont vaak een sterke *pad afhankelijkheid*, die niet alleen politiek is – politieke historie, politiek debat, politieke agenda's, et cetera – maar ook economisch en maatschappelijk. Veiligheidsproblemen kunnen als een grote dreiging worden gepercipieerd terwijl de dreiging relatief is, in termen van bijvoorbeeld waarschijnlijkheid. Bovendien worden de acties als gevolg van de gepercipieerde dreiging niet alleen politiek voortvarend ingezet, maar blijken ze ook economisch profijtelijk te zijn en maatschappelijk gedragen c.q. gewenst. Dat kan op verschillende manieren uitwerken.

In Israël wordt de proactieve aanpak van *cyber*dreigingen op die manier alomvattend en 'unstoppable'. De Israëlische overheid is bijvoorbeeld sterk afhankelijk geraakt van innovaties en beslissingen in/van de private sector. Terwijl in Duitsland de aanpak van migratie meer principieel dan pragmatisch is, en vooral ook legitimiteit – in plaats van hoofdzakelijk effectiviteit – vooropstelt, zowel vanwege de maatschappelijke gedragen FDGO-principes, als het feit dat vluchtelingen als economisch kapitaal (werknemers) gezien worden. Dat betekent dat 'de overheid' in onze vraagstelling relatief is. 'De overheid' is afhankelijk van economische en maatschappelijke krachten die niet zomaar te beteugelen zijn. Die krachten kunnen ook 'gebruikt' worden.

Dat neemt niet weg dat enige *beteugeling* mogelijk is, en dat 'de overheid' speelruimte heeft. Die is niet onverkort en vrijelijk aanwezig, juist vanwege de grotere economische en maatschappelijke krachten. Maar in relatie tot padafhankelijke invloeden kunnen overheden ruimte creëren, mits ze de *dilemma's* van de weerbare open samenleving voor ogen houden. Het omgaan met die dilemma's zit, zo concluderen we op grond van de landenstudies en vertaling naar Nederland, in de volgende *mechanismen* (zie ook onderstaande tabel).

Ten eerste, in beide cases gaat het niet enkel om het *pragmatisch* uitvoeren van bepaalde praktijken, maar ook om een *politiek debat* en vooral de *politieke framing* van de problematiek. In Israël en Duitsland wordt in politieke zin anders gekeken naar respectievelijk *cybersecurity* en het asiel- en migratievraagstuk dan in Nederland.

In de *framing* van een dreiging zit de genoemde pad afhankelijkheid, maar tevens keuzeruimte, als gevormde paden worden herkend en ter discussie gesteld.

Het omgaan met dreigingen vergt dat stil gestaan zal moeten worden bij de politieke *framing* van het probleem, in relatie tot economische en maatschappelijke krachten. In Israël gebeurt dat niet tot nauwelijks, in Duitsland veel meer.

Ten tweede, in beide cases zetten landen een bepaalde koers in, maar is het tevens van belang dat ze *alert* en *adaptief* zijn en blijven. Naarmate een overheid meer op weerbaarheid gaat sturen, en een stevige koers inzet, kan dit ten koste gaan van de flexibiliteit om beleid en uitvoering snel aan te passen, en de koers te verleggen. Dit maakt het lastiger om te anticiperen en te reageren op veranderingen, mede via het inzetten van personele en materiële capaciteit. Dat kan als *'weerbaarheidsparadox'* gezien worden. Naarmate de overheid meer in et op een specifieke weerbaarheid, wordt de weerbaarheid minder als zich nieuwe, onvoorspelbare ontwikkelingen voordoen. Vooral in de Israëlische casus wordt duidelijk dat de aanpak van *cyber*dreigingen een relatief autonoom proces is geworden. In Duitsland daarentegen is er meer ruimte voor *'trial and error'*.

Ten derde, in beide cases en vooral in de Duitse casus zoeken overheden naar een balans tussen *stimuleren en regisseren*. In de Israëlische casus ligt de nadruk vanuit de overheid vooralsnog vooral op het stimuleren van innovaties waarbij beperkte aandacht is voor mogelijke gevolgen van deze ontwikkelingen voor privacy, mensenrechten, et cetera. Het toegaan naar een regierol vanuit de Israëlische overheid, waarbij de overheid de kaders bepaalt in termen van het behoud van de waarden van de democratische rechtsstaat, zal binnen de Israëlische context niet makkelijk zijn. Veel bedrijven hebben zich er gevestigd om van het economische klimaat te profiteren. Bovendien trekt de *cybersecurity*sector ook nog eens veel geld naar zich toe middels Europese Horizon 2020 financiering. Het economische belang van deze sector is groot.

Nederland lijkt juist de nadruk te leggen op *regie* en *regulering*. De vraag in Nederland is dan ook meer, hoe kun je innovatie op het gebied van *cybersecurity* stimuleren met behoud van regie en controle? Bij regisseren hoort ook leren alsmede het borgen van de benodigde 'checks and balances'. In Israël zijn de 'checks and balances' in termen van het borgen van de democratische waarden, zoals we lieten zien, beperkt aanwezig. Dit kan (nog) minder worden met het nieuwe wetsvoorstel de *Cyber Security and National Cyber Directorate Bill.* Daarbij krijgt de Israeli National Cyber Directorate (INCD) een vergaande uitbreiding van de bevoegdheden op het gebied van *online* toezicht en dataverzameling, bij zowel overheidsorganisaties als private bedrijven, om een 'cyberattack' te voorkomen of te bestrijden. Volgens sommige critici roept het wetsvoorstel het beeld op van het INCD als 'overheids-spionageapparaat'.
In Duitsland zijn de *basiswaarden* van de democratische rechtsstaat steviger verankerd in het denken en doen van de overheidsdiensten en diverse correctiemechanismen voorhanden als het gaat om de omgang van betrokken overheidsdiensten met asiel en migratie.

Tabel 2. Sleutelmechanismen voor het gebalanceerd omgaan met weerbaarheid en openheid

Mechanismen	**Toelichting**
1. *Framing*	Duiding, eigen verhaal, open blik, *in relatie tot* (landspecifieke) context en pad afhankelijkheid
2. *Adaptiviteit*	Flexibiliteit, capaciteit, 'trial and error', *in relatie tot* koersvastheid en daadkracht
3. *Regie*	Principes, experimenteren, leren, 'checks and balances', *in relatie tot* partners en regels

8.5 AANBEVELINGEN VOOR HET VERSTERKEN VAN DE WOS

Op grond van de voorgaande hoofdstukken, alsmede de analyses en conclusies, willen we een aantal concrete aanbevelingen doen die voor overheden van belang zijn in het toewerken naar een WOS. We doen dat op basis van het *analysekader* zoals gepresenteerd in hoofdstuk 2. Daarbij kijken we naar de aspecten dreigingsperceptie en veiligheidspraktijken, waarbij waarden en belangen betrokken worden via onze nadruk op de balans tussen weerbaarheid en openheid. Verder doen we dat 'actiegericht', waarbij we ons bewust zijn van de afhankelijkheden waar overheden zich in bevinden, alsmede de grotere krachten die de aanpak van (on)veiligheid en dreiging omgeven.

Dreigingsperceptie

1 *Wees realistisch en relativeer, accepteer dat niet alle dreigingen het hoofd kunnen worden geboden.* De overheid zal eerlijk moeten zijn over het feit dat niet alle potentiële dreigingen kunnen worden weggenomen of voorkomen. Zij kan daarin de volgende keuze maken: ofwel een minimalistische veiligheidspreventie (dit garanderen wij, en verder niet); ofwel een uitgebreide veiligheidspreventie (dit garanderen wij, maar dan kost het ook extra capaciteit). Deze keuze bepaalt ook de interventiecapaciteit van de overheid: waar mag én kan wel of niet worden ingegrepen.

2 *Houd de monitoring rond dreigingspercepties goed in het oog.* Om een strategie te ontwikkelen waarin overheidsinstanties adequaat kunnen anticiperen op het dynamische veld van dreigingspercepties is het noodzakelijk om goed zicht te houden op de uiteenlopende en veranderende percepties. Deze worden onder andere in kaart gebracht in de Veiligheidsmonitor van het CBS en in de Risico en Crisisbarometer van de NCTV. Alleen op die manier kan de sociale constructie rondom een bepaalde dreiging begrepen worden, en kan de overheid zorgen voor een verhaal – *framing* – bij haar beleidsplannen en -praktijken dat als legitiem wordt beschouwd door de burgers.

3 *Wees voorbereid, ontwikkel een strategie om op wisselende dreigingspercepties te anticiperen*. Op basis van de monitoring is het mogelijk om voor de beleidsplannen en -praktijken te achterhalen of het verhaal achter het genomen risico (denk aan: de plaatsing van een AZC in een woonwijk) uitgelegd kan worden aan de burgers.

4 Om legitiem te kunnen zijn moeten beleidsplannen en -prakijken in overeenstemming zijn met wat de burgers ervan verwachten.
5 *Sta open voor verschillende percepties en principes*. Sommige burgers zijn bezorgd of hebben angst voor zaken die zij als bedreigend zien. Soms kunnen zij daaraan luid uiting geven. Weeg af of het mogelijk is of dat in respectvolle dialoog over dreigingspercepties gesproken kan worden waarbij zowel de zorgen en angsten worden geadresseerd als fundamentele principes van mensenrechten en openheid. Houd rekening met *onderstromen*, die niet alleen verzet tegen veranderingen impliceren, maar ook positieve houdingen.
6 *Maak jezelf en anderen bewust, werk aan veiligheidsscholing en educatie.* Joubert et al. (2015) betogen dat het onderwijs dé plek is om rechtstatelijke en democratische waarden over te dragen, een argument dat in de politieke discussie over de weerbare open samenleving ook terug te vinden is. Via educatie kunnen burgers en professionals in (publieke en private) organisaties meer reflectievermogen en handelingsperspectieven ontwikkelen zodat zij ook daadwerkelijk hun eigen verantwoordelijkheid kunnen nemen. De *cybersecurity* casus laat zien dat het van belang is om over de volle breedte te investeren in *human capital.* Dit betekent dat de focus ligt op het kwantitatieve deel: ICT-educatie en training voor jongeren en het kwalitatieve deel: behoud van hoogwaardige kennis in Nederland. Met het kwalitatieve deel wordt gehoor gegeven aan de oproep van Bos, Eeten en Jacobs (2017) om *brain drain* een halt toe te roepen.

Veiligheidspraktijken in reflectie op waarden

1 *Wees legitiem, zoek naar steun en draagvlak.* Balanceren vraagt om legitimeren, bijvoorbeeld aangaande de mate waarin we de rechten van het individu inperken in het geval van een crisis. In de ambtelijke voorbereiding zou dat expliciet meegewogen moeten worden, voordat overheden en partners vooral in een actie-modus terecht komen. In meer algemene zin geldt, wees principieel waar mogelijk. ‘Te pragmatisch’ en te daadkrachtig en effectief handelen kent een keerzijde.
2 *Maak expliciete afwegingen voorafgaand aan de inzet van maatregelen*. De Nederlandse governance-structuur rondom c*ybersecurity* wordt door respondenten regelmatig geprezen. Dit geeft dit vooral aan dat Nederland goed op orde heeft welke actor in welke crisissituatie voor welke taak verantwoordelijk is. Dit geeft echter nog weinig input voor de lastige afwegingen die gemaakt moeten worden gedurende een crisis in termen van inzet en mogelijke uitbreiding van bevoegdheden en de mogelijke effecten die dit zal hebben voor de weerbare open samenleving. In het geval van een crisis wordt van de overheid verwacht dat zij het voorliggende probleem oplost. Voor de overheid is het dan belangrijk om te weten welke acties er moeten worden ondernomen en op welke manier dit wordt uitgelegd. Het is daartoe van belang om op voorhand een heldere boodschap voorhanden te hebben, zodat betrokken actoren weten welk signaal er vanuit de overheid wordt gegeven in het geval van een bepaalde crisis. Om dit goed te kunnen doen, is het belangrijk om scenario’s van potentiële crises uit te denken.

3 Daarbij hoort het in kaart brengen van de (mogelijk uiteenlopende) dreigingspercepties, het anticiperen op de mogelijke reacties vanuit de maatschappij op verschillende crises en daaraan gekoppeld de reactie op de inzet van verschillende veiligheidspraktijken.[50]
4 *Hou ook in evaluerende zin zicht op de legitimiteit van het beleid.* Het is van belang vooraf na te denken in hoeverre beleid gedragen zal worden. Maar het is uiteraard ook van belang de daadwerkelijke ontvangst van maatregelen te meten zodra een maatregel in praktijk is gebracht. Dit soort metingen van legitimiteit richten zich op het maatschappelijk vertrouwen (percepties van burgers) in bepaald beleid en bepaalde instituties. Om legitiem te zijn is echter meer nodig dan alleen draagvlak onder burgers. Er is ook altijd reflectie nodig op soms conflicterende waarden en belangen: bijvoorbeeld over aan wie de voordelen toevallen en wie de kosten betalen. Daarbij spelen altijd de fundamentele principes van de rechtstaat een belangrijke rol. In de WOS betekent 'openheid' ook openheid aangaande de wijze waarop weerbaarheid wordt georganiseerd.

8.6 SLOTBESCHOUWING

Het beschermen van de waarden en belangen van de weerbare open samenleving (WOS) vraagt om een balanceer act van overheidsdiensten. Van de overheid wordt verwacht dat zij de samenleving beschermt tegen dreigingen. Dat moet krachtig, zichtbaar en op het eerste gezicht ferm dan wel 'met harde hand', maar naarmate de acties fermer en 'harder' zijn wordt de onveiligheidsperceptie aangejaagd en de openheid en vrijheid van ons type samenleving op de proef gesteld, dan wel aangetast. De diensten staan daarmee voor een lastige, schijnbaar dilemmatische opgave. Zeker omdat de dreigingen veelvuldig en fluïde zijn, en de dreigingsperceptie binnen de samenleving sterk varieert. Het is dan per land afhankelijk van de dreigingsperceptie en de beschermwaardig geachte waarden en belangen welke veiligheidspraktijken nodig en acceptabel worden geacht. Het vergt een *gevoelige* en *goed afgestemde governance* om hiermee om te kunnen gaan.

Dit start met het besef dat het niet om dilemma's maar om *paradoxen* gaat. Weerbaarheid en openheid staan niet naast of tegenover elkaar, maar kunnen op elkaar betrokken worden. Het vraagt vervolgens om een hoge mate van sensitiviteit voor mogelijke dreigingen en voor het zoeken naar overeenstemming tussen de betrokken actoren over die dreigingen. Dat vergt een goede antenne van regisserende diensten voor uiteenlopende meningen over dreigingen en over de wijzen waarop ze aangepakt zouden kunnen c.q. moeten worden. Verder vraagt het om reflectie, zowel ex-ante als ex post, op het handelen van betrokken diensten in het omgaan met deze dreigingen. Dit gaat zowel over welke instrumenten nodig zijn om de dreiging het hoofd te bieden, als om de daadwerkelijks inzet ervan en hoe deze door de samenleving ontvangen zal worden. Daarbij staat telkens de vraag centraal welke waarden en belangen verdedigd moeten worden en of de ingezette middelen te *legitimeren* zijn met het oog op dit doel.

---

[50] Zoals aangekondigd in de Cyber Security Agenda zal de Nederlandse overheid het Nationaal Crisisplan uitval ICT actualiseren.

In de weerbare open samenleving moet krachtig gehandeld worden, maar worden vragen gesteld, gemaakte afwegingen besproken, en onafhankelijke toetsing alsmede kritische reflecties gegarandeerd.

Bijlagen

KERNTEAM

Prof. dr Mirko Noordegraaf (expertise: management en professionals) (formeel projectleider) Mirko Noordegraaf is als hoogleraar Publiek Management verbonden aan departement Bestuurs- en Organisatiewetenschap (USBO). Hij is tevens vice-decaan van de faculteit Recht, Economie, Bestuur en Organisatie (REBO) en voorzitter van de leerstoelgroep Public Governance & Management (PGM). In zijn onderzoek richt hij zich op organisatie- en managementvraagstukken in publieke domeinen, met een nadruk op publieke managers en professionals in uiteenlopende sectoren.

Dr Marie-Jeanne Schiffelers (uitvoerend projectleider)
Marie-Jeanne Schiffelers is senior-adviseur/onderzoeker en is sinds 1998 verbonden aan USBO Advies. In deze functie heeft zij ruime ervaring opgedaan met het leiden en uitvoeren van (beleids)onderzoek en –evaluaties binnen de publieke sector in het algemeen en de sector Veiligheid en Justitie in het bijzonder. Veel onderzoeken waaraan zij meewerkte of waarover zij de leiding had, waren beleidsevaluaties in opdracht van diverse departementen of aan de overheid gelieerde instellingen.

Dr Karin Geuijen
Karin Geuijen is universitair docent aan het departement Bestuurs- en Organisatiewetenschap (USBO). Haar onderzoeksbelangstelling ligt bij multilevel en multisector netwerksamenwerking ten behoeve van het creëren van maatschappelijke meerwaarde (public value), met name op het terrein van justitie en veiligheid, en nog specifieker migratie en asielbeleid.

Dr Paulien de Morree
Paulien de Morree is als universitair docent verbonden aan het Instituut voor staatsrecht, bestuursrecht en rechtstheorie van de Universiteit Utrecht (UU). In oktober 2016 promoveerde zij op een onderzoek naar het verbod van misbruik van recht in het Europees Verdrag voor de Rechten van de Mens (EVRM), waarin de thematiek van een weerbare democratie een belangrijke rol speelde (*Rights and wrongs under the ECHR: The prohibition of abuse of rights in Article 17 of the European Convention on Human Rights*, Antwerpen: Intersentia, 2016.

Prof. dr Jacco Pekelder
Jacco Pekelder is universitair hoofddocent Geschiedenis van de Internationale Betrekkingen aan de Universiteit Utrecht en honorair professor Contemporary History of Western Europe aan de Universität des Saarlandes, Saarbrücken (D). Zijn onderzoek gaat onder meer over de sociale en politieke dynamiek van terrorisme, in het bijzonder over de confrontatie tussen de Bondsrepubliek en het linkse Duitse terrorisme van de Rote Armee Fraktion tussen 1968 en 1998.

EXPERTTEAM

Prof. dr Kees ten Bos (expertise: sociale psychologie van dreiging)
Kees van den Bos is sinds 2001 hoogleraar Sociale Psychologie met inbegrip van de Sociale Psychologie van de Organisatie (Faculteit Sociale Wetenschappen) en sinds 2013 hoogleraar Empirische Rechtswetenschap (Faculteit Recht, Economie, Bestuur en Organisatie).

Prof. dr Beatrice de Graaf (expertise: contra-terrorismebeleid)
Beatrice de Graaf is als hoogleraar History of International Relations and Global Governance verbonden aan de Universiteit Utrecht. Zij is hoofd van de afdeling Geschiedenis van de Internationale Betrekkingen. De Graaf's overkoepelende onderzoeksthema is de geschiedenis van veiligheid en (contra)terrorisme in de 19e tot 21e eeuw.

Prof. dr Paul 't Hart (expertise: leiderschap, bestuur en bestuur)
Paul 't Hart is hoogleraar Bestuurskunde aan de Utrechtse School voor Bestuurs- en Organisatiewetenschappen van de Universiteit Utrecht en co-decaan van de Nederlandse School voor Openbaar Bestuur. Ook is hij langdurig parttime verbonden aan het National Defence College van Zweden en de Australia New Zealand School of Government (ANZSOG). Zijn expertise ligt op het gebied van politiek-bestuurlijke beleids- en besluitvorming, politiekambtelijke verhoudingen, publiek leiderschap, publieke verantwoording en crisismanagement.

Prof. dr Henk Kummeling (expertise: de rol van grondrechten en noodrecht)
Henk Kummeling is sinds 1995 als hoogleraar staatsrecht en vergelijkend staatsrecht verbonden aan het Instituut voor staats- en bestuursrecht van de Universiteit Utrecht (UU). Van 1 september 2008 tot 1 september 2014 was hij decaan van de faculteit Recht, Economie, Bestuur en Organisatie van de UU. In 2015 benoemde het college van bestuur hem tot universiteitshoogleraar. In 2018 werd hij de rector magnificus van de UU. Kummeling publiceerde over diverse onderwerpen, zoals grondrechten, rechtsbescherming in de Europese Unie, openbaarheid van bestuur, politiek staatsrecht, en internationaal recht.

OVERZICHT RESPONDENTEN

Casus Duitsland

Organisatie	Gesprekspartner(s)	Datum
Pro Asyl, Frankfurt, Hessen	Dhr. K. Kopp	6 april 2018
Bundeskriminalamt, Wiesbaden, Hessen	Mr. H. Neumann, Dhr. M. Lechner en Mevr. Leibold	30 mei 2018
Landeskriminalamt, Wiesbaden, Hessen	Mr. S. Thurau	30 mei 2018
Bundesamt für Migration und Flüchtlinge, Nürnberg, Beieren	Dhr. M. Klemm en mevr. M. Uhlmann, MSc	7 juni 2018
Institut für Demokratie und Zivilgesellschaft, Jena, Thüringen	Dr. M. Quent	3 juli 2018

Casus Israël

Organisatie	Gesprekspartner(s)	Datum
National Cyber Directorate, Tel Aviv	Dhr. H. Mei-Zahav MBA, Mr. A. Ashkenazy en Mr. R. Yamin	19 mei 2018
Cyber Security, Ministry of Foreign Affairs, Jerusalem	Dhr. I. Moed MSc	12 mei 2018
Tel Aviv University, Tel Aviv	Dhr. L. Tabansky MA	19 mei 2018
CSCSS, Tel Aviv	Dhr. D. Norwell BSc	16 mei 2018
Cisco ISR, Tel Aviv	Mevr. Z. Abzuk MSc	17 mei 2018 (focusgroep 1)
CyKicks, Tel Aviv	Mr. R. Raz	17 mei 2018 (focusgroep 1)
CyberSpark, Tel Aviv	Dhr. R. Zehavi MSc	17 mei 2018 (focusgroep 1)
Holom Institute for Technology Tel Aviv	Dr. H. Menashri	17 mei 2018 (focusgroep 2)
Layer7Defense, Tel Aviv	Mr. D. Chema	17 mei 2018 (focusgroep 2)

Frimitas, Tel Aviv	Mr. R. Efrati	17 mei 2018 (focusgroep 2)
CyberRisk, Tel Aviv	Dhr. E. Harari	17 mei 2018 (focusgroep 2)
Comsec, Tel Aviv	Dhr. G. Cohen BSc	17 mei 2018 (focusgroep 2)
Consienta, Tel Aviv	Dhr. G. Dagan MSM MBA	17 mei 2018 (focusgroep 2)
Cyber Together, Tel Aviv	Dhr. A. Refaeli BA	17 mei 2018 (focusgroep 2)

Vertaalslag

Organisatie	**Gesprekspartner(s)**	**Datum**
Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag	Prof. dr. C. Prins en dr. R. Passchier	20 augustus 2018
Migratie (voormalig), Centraal Orgaan opvang Asielzoekers (voormalig), Den Haag	Drs. J. Goet	21 augustus 2018
Adviesraad voor wetenschap, technologie en innovatie, Den Haag	Prof. dr. U. Rosenthal	28 augustus 2018
Rijksinstituut voor Milieu en Veiligheid, Bilthoven	Dhr. L. Gooijer MSc	28 augustus 2018
VluchtelingenWerk Nederland, Amsterdam	Dhr. J. Kuipers MSc	29 augustus 2018
Nationaal Cyber Security Centrum, Den Haag	Mr. H. De Vries	29 augstus 2018
Universiteit Leiden, politicologie, tevens Crisisplan BV	Prof. dr. A. Boin	30 augustus 2018
Centraal Orgaan opvang Asielzoekers, Den Haag	Drs. J. Helder en dhr. J. van der Have	30 augustus 2018

TOPICLIJST ASIEL- EN MIGRATIECASUS DUITSLAND

„Forschungsprojekt Wehrhafte Offene Gesellschaft“

I Forschungsprojekt

Dieses Forschungsprojekt wird von der Universität Utrecht im Auftrag des Zentrums für wissenschaftliche Forschung und Dokumentation des niederländischen Ministeriums für Justiz und Sicherheit (WODC) und des Nationalen Koordinators für Terrorismusbekämpfung und Sicherheit (NCTV) durchgeführt. Ziel der Forschung ist es, Erkenntnisse darüber zu gewinnen, mit welchen Maßnahmen potenzielle Bedrohungen rechtzeitig verhindert werden können, um die offene Gesellschaft mit ihren demokratischen und konstitutionelle Werten zu schützen.

II Bedrohungen

- Welche Bedrohungen (und evt. schwache Indikatoren oder „weak signals“) im Bereich der Asyl- und Migrationsfragen werden politisch, administrativ und gesellschaftlich als Schwerpunkt behandelt?
- Welche Situationen und Gruppen bzw. Personen werden von Ihrer Organisation als potenzielle Bedrohungen betrachtet?
- Wie verhalten diese Bedrohungen sich zueinander?
- Wie reagiert Ihre Organisation auf diese Bedrohungen (präventiv und kurativ)?
- Wie reagieren Politik und Gesellschaft auf diese potenzielle Bedrohungen?
- Wie geht Ihre Organisation mit diesen politischen und gesellschaftlichen Reaktionen um?

III Interessen

- Welche Interessen (Werte der deutschen Gesellschaft) werden von diesen potenziellen Bedrohungen bedroht?

VI Maßnahmen

- Welche Möglichkeiten sehen Sicherheitsexperten im Bereich der (technologischen) Maßnahmen um diese potenzielle Bedrohungen möglichst früh zu erkennen?
- Werden die Maßnahmen nur von Sicherheitsbehörden durchgeführt oder sind auch private Organisationen beteiligt?
- Inwieweit können Sicherheitsbehörden von privaten Organisationen lernen, was frühzeitiger Erkennung potenzieller Bedrohungen angeht?
- Sind die Organisation und die Koordination der beteiligten Organisationen an der Einschätzung dieser potenziellen Bedrohungen angepasst?
- Könnten Sie mir andeuten, welche Kapazitäten Ihrer Einschätzung nach für eine erfolgreiche Prävention bzw. Reaktion was den (potentiellen) Bedrohungen angeht, notwendig wären?

V Auswirkungen

- Welche Auswirkungen haben die oben angesprochenen Maßnahmen hinsichtlich der demokratischen und rechtsstaatlichen Werten der deutschen Gesellschaft?
- Spezifisch zu den demokratischen Werten:
    - Wie ist die Verantwortung ihrer Organisation gegenüber den politische Verantwortlichen (Personen und Instanzen) geregelt?
    - Welche internen Verfahren gibt es in Ihrer Organisation, mit denen bereits im Vorfeld der oben genannten Verantwortung die Respektierung der demokratischen Grundwerte möglichst gesichert wird?
- Spezifisch zu den rechtsstaatlichen Werten:
    - Auf welche Weise, ist der Schutz der Grundrechte der betroffenen Asylbewerber bzw. Flüchtlinge in Ihrer Arbeit zum Schutz der deutschen Sicherheit integriert?
    - In wie weit steht den Betroffenen an allen Momenten, an denen Ihre Organisation sich mit ihnen beschäftigt, noch dem Rechtsgang zu?
- Was ist das „höhere“ gesellschaftliche Interesse, das Ihre Organisation am Ende schützt?

VI Quellen

- Welche zusätzlichen Quellen/Personen/Instanzen empfehlen Sie uns zu konsultieren?

TOPICLIJST CYBERSECURITY CASUS ISRAEL

"Research Project Resilient Open Society"

I Introduction

- Introduction: researcher, research (see below), and respondent.
- Recording: request to record the conversation.
- Traceability of data: name of respondent is attached but quotations are not traceable in the final report.

This research is carried out by Utrecht University on behalf of the Research and Documentation Center of the Dutch Ministry of Justice and Security, and the National Coordinator for Security and Counterterrorism. The aim of the research is to gain insights into security practices that can solve potential threats, in order to protect the open society and its democratic values (e.g. human rights).

II Threats

- Which threats are debated in parliament and in public (political and societal discourse)?
- Which groups/persons are perceived as potential threats to the State of Israel?
- In what way might these threats have a negative impact on the democratic and constitutional values of the State of Israel according to the political and societal debates?
- How does your organization deal with the political and societal reactions to these perceived threats? And how does your organization respond to these threats?

III Values

- What values does the State of Israel aim to protect with their cyber security policy?
- What values does your organization consider to be worthwhile to protect?

IV Practices

- What possibilities do experts (including private companies) see to recognize these perceived threats as early as possible?
- Who carries out security practices in the State of Israel (e.g. the government, public organizations, or private companies)?
- How are security practices operationalized in the State of Israel (who's is responsible for what; and is there any cooperation between public and private organizations?)
- What lessons can be learnt from private cyber security companies when it comes to anticipating to (potential) threats?

V Effects

- What are the effects of these security practices on the democratic values of the State of Israel?
  CONSIDER THE FOLLOWING QUESTIONS:

PUBLIC ORGANIZATIONS

- What security practices are carried out by the National Cyber Directorate (NCD)?
- What is the reason that the National Cyber Bureau (NCB) and National Cyber Security Authority (NCSA) are merged in 2017?
- Who supervises the National Cyber Directorate?
- In what way is the National Cyber Directorate controlled by the parliament of the State of Israel?
- To what extent does the National Cyber Directorate share information with the parliament of the State of Israel, and what is kept secret?

PRIVATE COMPANIES

- What security practices are carried out by your company?
- What does your company do to protect the privacy of the users of your products?
- What do customers think about your products? Do they feel that their privacy is protected?
- Are there any laws and regulations in the State of Israel to protect the privacy of your customers; and in what way does the State of Israel control whether your company acts according to the law?

NGOs

- What are the main concerns of NGOs regarding cyber security?
- How do authorities react to these concerns?
- To what extent are NGOs able to address these concerns in court?

V Additional sources

- What additional sources (e.g. literature and respondents) would you advise us to read/contact to answer our research question?

TOPICLIJST VERTAALSLAG NEDERLAND

I Kennismaking en huishoudelijke mededelingen

- Voorstelronde
- Gesprek van 1 uur (check bij respondent)
- Herleidbaarheid gegevens: naam respondent komt in bijlage maar citaten niet herleidbaar in rapport. Bevindingen worden op hoger aggregatieniveau opgenomen.
- Eventueel verzoek tot het opnemen van het gesprek.

II Introductie op onderzoek

In opdracht van het Wetenschappelijk Onderzoek en Documentatiecentrum van het Nederlandse ministerie van Justitie en Veiligheid en de Nationaal Coördinator Terrorismebestrijding en Veiligheid voert de Universiteit Utrecht een onderzoek uit ten behoeve van het opstellen van een 'toekomstvisie op weg naar een weerbare samenleving'. Doel van het onderzoek is het verkrijgen van inzicht in welke maatregelen ingezet kunnen worden om aan (snel) veranderende dreigingen op tijd het hoofd te kunnen bieden om de open samenleving met haar democratische en rechtsstatelijke waarden (waaronder mensenrechten) te kunnen beschermen.

De centrale vraag hierbij is:

➢ *Hoe kan de overheid dreigingen/verstoringen vanuit de omgeving voor de weerbare open samenleving detecteren en duiden, om hier (in een zo vroeg mogelijk stadium en in onderlinge samenhang) op een gebalanceerde wijze op te kunnen reageren, om zodoende de open samenleving met haar democratische en rechtsstatelijke waarden te beschermen?*

Doel van het onderzoek is bouwstenen aandragen voor een nationale toekomstvisie. Daartoe zoomen we in op een tweetal specifieke problematieken te weten asiel en migratieproblematiek/*cybersecurity*.

We zouden in dit gesprek graag met u van gedachten wisselen over de dreiging voor Nederland op het vlak van Asiel en migratieproblematiek/ *Cybersecurity* voor de samenleving, over opgedane inzichten vanuit Duitsland/Israël m.b.t. de betreffende casus en de bruikbaarheid ervan voor de Nederlandse situatie, over in te zetten maatregelen om de dreiging te begrenzen en over de mogelijke gevolgen ervan voor de weerbare open samenleving waarin het gaat om een samenspel van veiligheid, weerbaarheid, en waarden behorende bij de open samenleving, zoals rechtsstatelijke en democratische waarden (analysemodel achter de hand houden).

III Dreigingen

- Op welke dreigingen (en weak signals) liggen in Nederland m.b.t. asiel en migratie/*cybersecurity* de politieke, bestuurlijke en maatschappelijke focus?

- Dreigingsperceptie: welke situaties en/of personen worden vanuit uw organisatie gepercipieerd als potentiële dreigingen?
- Hoe reageren de politiek en de samenleving op deze potentiële dreigingen; In hoeverre is deze reactie vanuit optiek (on)wenselijk?
- Welke reactie zou u graag zien vanuit welke stakeholders en waarom?

IV Beschermwaardige belangen

- Welke beschermwaardige belangen worden bedreigd door verstoringen die gerelateerd zijn aan asiel- en migratieproblematiek/*cybersecurity*?
- Wat is de dreiging en waarvoor is het precies een dreiging?

V Praktijken

- Hoe kijkt u naar de Duitse/Israëlische casus? (Voor beknopte toelichting zie kader). Wat kan Nederland hiervan leren?
- Wat is de wenselijkheid/uitvoerbaarheid van de gehanteerde maatregelen voor Nederland?
- Welke mogelijkheden ziet u voor de Nederlandse situatie om met (technologische) maatregelen, disruptieve maatschappelijke ontwikkelingen dreigingen eerder te voorzien? Welke stakeholders zijn daarbij van belang en in welk opzicht?
- Welke maatregelen vergen de vaak fluïde dreigingen rondom asiel en migratie/*cybersecurity* voor de organisatie van de maatregelen?
- Welke gevolgen hebben de fluïde dreigingen voor de organisatie van de maatregelen?
  a In hoeverre kunnen publieke organisaties leren van private organisaties als het gaat om te kunnen anticiperen op snelle veranderingen?
  b Wat kunnen deze snelle veranderingen betekenen voor de samenhang tussen de verschillende actoren?
  c Wat kunnen de snel veranderende dreigingen betekenen voor (afstemming tussen) werkprocessen van de betrokken organisaties die verantwoordelijk zijn voor het veiligheidsbeleid onder meer als het gaat om agendering en besluitvorming?
  d Kunnen indicaties worden gegeven van capaciteiten zowel kwantitatief als kwalitatief (competenties) die nodig zijn om de weerbaarheid te versterken?

VI Effect van de praktijken voor de WOS

- Wat zijn de effecten van de gehanteerde praktijken rondom asiel en migratieproblematiek in Duitsland en *cybersecurity* in Israël in uw optiek voor de democratische en rechtsstatelijke waarden en institutionele weerbaarheid?
- Welke problemen ziet u voor de Nederlandse balans tussen weerbaarheid en openheid wanneer de Duitse/Israëlische aanpak gevolgd wordt?
- Welke balans tussen weerbaarheid en openheid acht u wenselijk voor de Nederlandse situatie en hoe kan daaraan gewerkt worden?

REFERENTIES PER HOOFDSTUK

Hoofdstuk 1

Clingendael (2017). Clingendael Strategische Monitor 2017. Verkregen via: https://www.clingendael.org/pub/2017/monitor2017/

De Graaf, B. (2013) Taming the future? Een historisch perspectief op de omgang met nieuwe risico's en onzekerheid. In: De Graaf, B., Brenninkmeijer, A., Roeser, s., Passchier, W. (eds.), Omgaan met omgevingsrisico's en onzekerheden. Hoe doen we dat samen? Essaybundel, pp. 20 – 47.

Garland, D. (2001). The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: University of Chicago Press.

Kamerstukken II, 2015-2016, 30 821, nr. 32.

Kamerstukken II, 2017-2018, 33 763, nr. 141.

Ministerie van Buitenlandse Zaken (2018). Beleidsnota Investeren in Perspectief. Verkregen via: https://www.rijksoverheid.nl/documenten/beleidsnota-s/2018/05/18/pdf-beleidsnota-investeren-in-perspectie

Ministerie van Buitenlandse Zaken (2018). Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022. Den Haag: Ministerie van BuZa.

Ministerie van Defensie (2018). Defensienota 2018. Investeren in onze mensen, slagkracht en zichtbaarheid. Verkregen via: https://www.defensie.nl/downloads/beleidsnota-s/2018/03/26/defensienota-2018

Ministerie van Economische Zaken en Klimaat (2018). Nederlandse digitale agenda. Verkregen via: https://www.rijksoverheid.nl/onderwerpen/ict/ict-en-economie/nederlandse-digitale-agenda

Ministerie van Justitie en Veiligheid (2018). Nederlandse Cybersecurity Agenda. Verkregen via: https://www.ncsc.nl/organisatie/nederlandse-cybersecurity-agenda.html

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2015). Voortgangsbrief nationale veiligheid. Verkregen via: https://www.nctv.nl/binaries/voortgangsbrief-nationale-veiligheid-12-mei-2015_tcm31-29624.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). Nationale Contraterrorismestrategie 2016-2020. Verkregen via: https://www.nctv.nl/binaries/CT-strategie%202016-2020_tcm31-80007.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). Nationaal Handboek Crisisbesluitvorming. Verkregen via: https://www.nctv.nl/binaries/Nationaal%20Handboek%20Crisisbesluitvorming_tcm31-32327.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). Nationaal Veiligheidsprofiel 2016. Verkregen via: https://www.nctv.nl/binaries/Nationaal%20Veiligheidsprofiel%202016_tcm31-232083.pdf
Nationaal Cyber Security Centrum (2017). Cybersecuritybeeld Nederland. Verkregen via: https://www.ncsc.nl/?f=37

Rijksinstituut voor Veiligheid en Milieu (2016). Nationaal Veiligheidsprofiel 2016. Verkregen via: https://www.rivm.nl/RIVM/Organisatie/Centra/Centrum_Veiligheid/Analistennetwerk_Nationale_Veiligheid/Nationaal_Veiligheidsprofiel_2016

Wetenschappelijke Raad voor het Regeringsbeleid (2017). Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid. Verkregen via: https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen

Hoofdstuk 2

Bergson, H. (1932). Les deux sources de la morale et de al religion. Paris: Flammarion.

Bourbeau, P. (2013). Resiliencism: premises and promises in securisation research. Resilience 1(1): 3-17.

Boin, A. (2017). De Grenzeloze Crisis: Uitdagingen voor Politiek en Bestuur. Verkregen via: https://openaccess.leidenuniv.nl/bitstream/handle/1887/61089/Oratie-Prof.-R.A.-Boin-1.pdf?sequence=1

Burkens, M., Kummeling, H, Vermeulen, B., Wildershoven, R. (2017). Beginselen van de democratische rechtsstaat. Inleiding tot de grondslagen van het Nederlandse staats- en bestuursrecht. Alphen aan de Rijn: Wolters Kluwer.

Buzan, B., Waever, O., Wilde, de, J. (1998). Security: A New Framework for Analysis. London: Lynne Riener Publishers.

Clingendael (2017). Clingendael Strategische Monitor 2017. Verkregen via: https://www.clingendael.org/pub/2017/monitor2017/

De Graaf, B. (2017). Heilige strijd. Het verlangen naar veiligheid en het einde van het kwaad. Utrecht: Boekencentrum.

De Graaf, B. (2014). Waar zijn wij bang voor? Een religieus-theologische benadering van veiligheid. Verkregen via: https://www.pthu.nl/actueel/nieuws/Nieuwspdf/defwaar-zijn-wij-bang-voor-rede-oaj-pthu.pdf

Geldof, D. (2013). Superdiversiteit. Hoe migratie onze samenleving verandert. Leuven: Acco Uitgeverij.

Kamerbrief over adviesrapport WRR (2018). Reactie op 'Veiligheid in een wereld van verbindingen'. Verkregen via: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/28/kamerbrief-over-adviesrapport-wrr-%E2%80%98veiligheid-in-een-wereld-van-verbindingen

Loewenstein, K. (1937a). Militant Democracy and Fundamental Rights, I. The American Political Science Review, 31(2): 417-432.

Loewenstein, K. (1937b). Militant Democracy and Fundamental Rights, II. The American Political Science Review, 31(4): 638-658.

Ministerie van Buitenlandse Zaken (2018). Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022. Den Haag: Ministerie van BuZa.

Nationaal Cyber Security Centrum (2017). Cybersecuritybeeld Nederland 2017: Digitale weerbaarheid Nederland blijft achter op groeiende dreiging. Verkregen via: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). Nationaal Veiligheidsprofiel 2016. Verkregen via: https://www.nctv.nl/binaries/Nationaal%20Veiligheidsprofiel%202016_tcm31-232083.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016). Voortgangsbrief 2016. Verkregen via: https://www.nctv.nl/binaries/Voortgangsbrief%20Nationale%20Veiligheid_tcm31-98709.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2007). Strategie nationale veiligheid. Verkregen via: https://www.nctv.nl/binaries/strategie-nationale-veiligheid-2007_tcm31-32502.pdf

Popper, K. (1945). Die offene Gesellschaft und ihre Feinde. Bern: Francke Verlag.

Regeerakkoord (2017). Vertrouwen in de toekomst. Verkregen via: https://www.rijksoverheid.nl/regering/documenten/publicaties/2017/10/10/regeerakkoord-2017-vertrouwen-in-de-toekomst

Overkamp, S., Tollenaar, A. (2013). Integraal veiligheidsbeleid en planverplichting. Bestuurswetenschappen, 67(4): 63-79.

Noordegraaf, M., Schiffelers, M., Douglas, S., Van Rossem, J., Terpstra, N. De Graaf, B., Kummeling, H. (2017). Nood breekt wet? Terroristische dreiging, noodtoestand en maatschappelijke effecten. Verkregen via: https://www.wodc.nl/binaries/2805_Volledige_Tekst_tcm28-294924.pdf

Rijksinstituut voor Veiligheid en Milieu (2016). Nationaal Veiligheidsprofiel 2016. Verkregen via: https://www.rivm.nl/RIVM/Organisatie/Centra/Centrum_Veiligheid/Analistennetwerk_Nationale_Veiligheid/Nationaal_Veiligheidsprofiel_2016

Stol, W., Rijpma, J., Tielenburg, C., Veenhuysen, H., Abbas, T. (2016). Basisboek Integrale Veiligheid. Bussum: Coutinho.

TNO (2014). Meetmethoden weerbaarheid. Verkregen via: https://www.wodc.nl/binaries/2342-samenvatting_tcm28-73072.pdf

Wetenschappelijke Raad voor het Regeringsbeleid (2017). Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid. Vekregen via: https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen

Hoofdstuk 3

Forbes (2017). Six reasons Israel became a cybersecurity powerhouse leading the $82 billion industry. Verkregen via: https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#2832fda1420a

Das Statistik Portal (2017). Zuwanderung nach Deutschland. Verkregen via: https://de.statista.com/statistik/daten/studie/28347/umfrage/zuwanderung-nach-deutschland/

Hoofdstuk 4

Akrap, D. (2015). Germany's response to the refugee crisis is admirable. But I fear it cannot last. Verkregen via: https://www.theguardian.com/commentisfree/2015/sep/06/germany-refugee-crisis-syrian

Alexander, R. (2018). *Die Getriebenen. Merkel und die Flüchtlingspolitik: Report aus dem Innern der Macht. Aktualisierte Ausgabe. München: Siedler Verlag.*

Arnold, S., Bischoff, S. (2016). 'Wer sind wir denn wieder? Nationale Identitäten in Krisenzeiten', *Aus Politik und Zeitgeschichte*, 14-15/2016, 'Zufluchtsgesellschaft', 4 april 2016: 28-34.

Becker, E. (2018). 'Die Moscheen sollen sich in Luft auflösen'. Frankfurt: *Frankfurter Allgemeine Zeitung*.

Braun, S., Fried, N. (2018). Merkel und Seehofer streiten wieder. Migrationspolitik. München: Süddeutsche Zeitung.

Bundesagentur für Arbeit, Satistik/Arbeitsmarktberichterstattung (2018). *Fluchtmigration, Berichte: Arbeitsmarkt kompakt*, April 2018. Verkregen via: https://statistik.arbeitsagentur.de/Statischer-Content/Statistische-Analysen/Statistische-Sonderberichte/Generische-Publikationen/Fluchtmigration.pdf

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2018). Geschichte. Verkregen via: https://www.bbk.bund.de/DE/DasBBK/Geschichte/geschichte_node.html

Bundesamt für Bevolkerungsschutz und Katastrophenhilfe (2018). Krisenmanagement. Verkregen via: https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/GMLZ/GMLZ_einstieg.html

Bundesamt für Migration und Flüchtlinge (2015). *Aktuelle Zahlen zu Asyl, Ausgabe: Dezember 2015, Tabellen, Diagramme, Erläuterungen*. Verkregen via: http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/Statistik/Asyl/aktuelle-zahlen-zu-asyl-dezember-2015.pdf?__blob=publicationFile

Bundesamt für Migration und Flüchtlinge (2018). Versuch der Einflussnahme von Rechtsextremisten auf Anti-Asyl-Kundgebungen des demokratischen Spektrums. Verkregen via: https://www.verfassungsschutz.de/de/aktuelles/schlaglicht/schlaglicht-2018-03-einflussnahme-von-rechtsextremisten

Bundeskriminalamt (2016). *Kriminalität im Kontext von Zuwanderung. Bundeslagebild 2015*. Wiesbaden: Bundeskriminalamt.
Bundeskriminalamt (2017). Presseinformation: Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern. RADAR-iTE (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus). Verkregen via: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html

Bundeskriminalamt (2018). Deliktsbereiche. Verkregen via: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/pmk_node.html
Bundeskriminalamt (2018). Polizeilicherstaatsschutz. Verkregen via: https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/PolizeilicherStaatsschutz/polizeilicherstaatsschutz_node.html

Bundesministerium des Innern (2017). Verfassungsschutzbericht 2016. Fakten und Tendenzen – Kurzzusammenfassung. Berlin: Bundesministerium des Innern.

Bundesministerium des Innern, für Bau und Heimat (2018). „Wer den Rechtsstaat ablehnt, kann keine Nachsicht erwarten", Verbot der rockerähnlichen Gruppierung "Osmanen Germania BC". Verkregen via: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/07/verbot-osmanen.html

Bundesministerium des Innern, für Bau und Heimat (2018). *Polizei 2020. – White Paper.* Verkregen via: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1

Bundeszentrale für politische Bildung (2018). Bevölkerung mit Migrationshintergrund I. In absoluten Zahlen, Anteile an der Gesamtbevölkerung in Prozent, 2016. Verkregen via: http://www.bpb.de/nachschlagen/zahlen-und-fakten/soziale-situation-in-deutschland/61646/migrationshintergrund-i

Bundeszentrale für politische Bildung (2018). Freiheitliche demokratische Grundordnung. Verkregen via: http://www.bpb.de/nachschlagen/lexika/pocket-politik/16414/freiheitliche-demokratische-grundordnung

Converso, S., Bron, F. (ND). *Twenty-four Hours at the Grandhotel Cosmopolis in Augsburg. Stories of Work, Migration, and Collectivity*. Verkregen via: http://www.on-curating.org/issue-30-reader/twenty-four-hours-at-the-grandhotel-cosmopolis-in-augsburg-stories-of-work-migration-and-collectivity.html

Conze, E. (2009). Die Suche nach Sicherheit. Eine Geschichte der Bundesrepublik Deutschland von 1949 bis in die Gegenwart. München: Siedler Verlag.

Der Bundeswahlleiter (2017). Pressemitteilung Nr.34/17. Verkregen via: https://www.bundeswahlleiter.de/info/presse/mitteilungen/bundestagswahl-2017/34_17_endgueltiges_ergebnis.html

Deutscher Bundestag, 'Drucksache 18/12752', 16 juni 2017.
Deutscher Bundestag. Drucksache 18/11546', 16 maart 2017.

Deutscher Bundestag. Drucksache 19/804. 20 februari 2018.

Deutschlandfunk Kultur (2018). Jeder vierte Geflüchtete bereits im Job. Verkregen via: https://www.deutschlandfunkkultur.de/integration-auf-dem-deutschen-arbeitsmarkt-jeder-vierte.1008.de.html?dram:article_id=419254

Diekmann, F. (2018). Eine Spur von Spurwechsel. Verkregen via: http://www.spiegel.de/wirtschaft/soziales/einwanderung-koalition-einigt-sich-auf-eine-spur-von-spurwechsel-a-1231171.html

DpolG (2018). 'Informationsaustausch zwischen den Sicherheitsbehörden wird endlich verbessert'. Verkregen via: https://www.dpolg.de/aktuelles/news/informationsaustausch-zwischen-den-sicherheitsbehoerden-wird-endlich-verbessert/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=f2c5f24b05845144abdd78c1c315bf7f

Eurostat (2016). Asylum in the EU Member States. Record number of over 1.2 million first time asylum seekers registered in 2015. Syrians, Afghans and Iraqis: top citizenships'. Verkregen via: http://ec.europa.eu/eurostat/documents/2995521/7203832/3-04032016-AP-EN.pdf/790eba01-381c-4163-bcd2-a54959b99ed6

Eurostat (2018). Full list of Member States' notifications of the temporary reintroduction of border control at internal borders pursuant to Article 25 et seq. of the Schengen Borders Code. Verkregen via: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/schengen/reintroduction-border-control/docs/ms_notifications_-_reintroduction_of_border_control_en.pdf

Frevel, B., Rinke, B. (2017). Innere Sicherheit als Thema parteipolitischer Auseinandersetzung. *Aus Politik und Zeitgeschichte*, 32-33/2017, 7 augustus 2017, 'Innere Sicherheit': 4-10.

Heber, G., Adamczyk, M. , Kochs, S. (2011). *Konzept für eine soziale Skulptur in Augsburgs Herzen*. Augsburg: Projektbüro „Grandhotel"

Jakob, C. (2016). 'Die Bleibenden. Flüchtlinge verändern Deutschland', *Aus Politik und Gesellschaft*, 14-15/2016, 'Zufluchtsgesellschaft Deutschland', 4 april 2016: 9-14.

Klimeniouk, N. (2016). 'Das Märchen aus Marzahn. Russlanddeutsche'. Frankfurt: *Frankfurter Allgemeine Zeutung*.

Knopp, D. (2018). Heimatministerium in Bayern – Was hat es gebracht? Verkregen via: https://www.br.de/nachricht/heimatministerium-fuer-bayern-was-hat-es-gebracht-100.html

Konar, Ö., Kreienbrink, A., Stichs, A. (2017). Zuwanderung und Integration. Aktuelle Zahlen, Entwicklungen, Massnahmen, *Aus Politik und Zeitgeschichte*, 27-29/2017, Integrationspolitik, pp. 13-20.

Kretschmann, A. (2017). Soziale Tatsachen. Eine wissenssoziologische Perspektive auf den "Gefährder". *Aus Politik und Zeitgeschichte*, 32-33/2017, 'Innere Sicherheit': 11-16.

Lohse, E., Wehner, M. (2018). 'Missglückte Vertuschung. Der Fall Amri'. Frankfurt: *Frankfurter Allgemeine Zeitung*.
Müller, O. en Pollack, D. (2017) Angekommen und auch wertgeschätzt? Integration von Türkeistämmigen in Deutschland, *Aus Politik und Zeitgeschichte*, 27-29/2017, Integrationspolitik, 3 juli 2017: 41-46.

Münkler, H., Münkler, M. (2016). *Die neuen Deutschen. Ein Land vor seiner Zukunft*. Bonn: Bundeszentrale für politische Bildung.

ProAsyl (2016). 'Rechtlichen Veränderungen für Geduldete. Verkregen via: https://www.proasyl.de/wp-content/upload/2015/12/Papier_RechtlicheVeränderungenfürGeduldete.pdf

Quent, M. (2016). Selbstjustiz im Namen des Volkes: Vigilantischer Terrorismus. *Aus Politik und Zeitgeschichte*, 24-25/2016, 'Terrorismus', 13 juni 2016: 20-26.

R+V Versicherung (2016). Sicherheit bedroht: Terror, Extremismus und Flu̇chtlingskrise dominieren die Ä̈ngste der Deutschen. Verkregen via: https://www.ruv.de/static-files/ruvde/downloads/presse/aengste-der-deutschen-2016/ruv-aengste-2016-ergebnisse.pdf

Rigoll, D. (2017). Streit um die Streitbare Demokratie. Ein Rückblick auf die Anfangsjahrzehnte der Bundesrepublik. Aus Politik und Zeitgeschichte, 32-33/2017, 7 augustus 2017, 'Innere Sicherheit': 40-45.

Schnell, L. (2018). 'Die wichtigsten Fragen und Antworten zum Polizeiaufgabengesetz'. München: Süddeutsche Zeitung.

Schröter, S. (2016). *'Gott näher als der eigenen Halsschlagader'. Fromme Mulsime in Deutschland.* Frankfurt: Frankfurter Neue Presse.

Schubert, S. (2018). 'Enthüllt: Wie das BKA bei der Flüchtlingskriminalität manipuliert'. Geraadpleegd via: https://kopp-report.de/enthuellt-wie-das-bka-bei-der-fluechtlingskriminalitaet-manipuliert/

Seehofer, H. (2018). Warum Heimatsverlust die Menschen so umtreibt. Frankfurt: Frankfurter Allgemeine Zeitung.

Sly, L. (2015). 8 reasons Europe's refugee crisis is happening now. Verkregen via: https://www.washingtonpost.com/news/worldviews/wp/2015/09/18/8-reasons-why-europes-refugee-crisis-is-happening-now/?noredirect=on&utm_term=.4e9ea79dc476

Spiegel (2018). Lange Haftstrafen für rechte Terrorgruppe Freital. *Spiegel Online*, 7 maart 2018, http://www.spiegel.de/panorama/justiz/dresden-gruppe-freital-terrorprozess-lange-haftstrafen-fuer-angeklagte-a-1196857.html
Statista (2017). Umfrage zu den wichtigsten themen im Wahlkampf zur Bundestagswahl in Deutschland. Verkregen via: https://de.statista.com/statistik/daten/studie/670815/umfrage/umfrage-zu-den-wichtigsten-themen-im-wahlkampf-zur-bundestagswahl-in-deutschland/

Taberner, S. (2017) "Grey" culture', in: Sarah Colvin (ed.), *The Routledge Handbook of German Politics and Culture* (London en New York 2015): 268-282.

The Economist (2018). Homeland insecurity. Germany's Heimat politics. New York: The Economist.

Tibi, B. (1996). 'Multikultureller Werte-Relativismus und Werte-Verlust', *Aus Politik und Zeitgeschichte*, 52–53/1996: 27–36.

Van de Poll, W. (2018). Vetes, chaos en zwendel bij de migrantendienst. Amsterdam: Trouw.

Vehlewald, H. (2018). Wie kriminell sind Zuwanderer wirklich?'. Hamburg: Bild.

Weise, V. (2018). BKA legt umfangreichen Bericht zur Kriminalität von Zuwanderern vor. Hamburg: Die Welt.

Hoofdstuk 5

Alink, F.B. (2006) Crisis als kans? over de relatie tussen crises en hervormingen in het vreemdelingenbeleid van Nederland en Duitsland, Vossiuspers UvA - Amsterdam University Press,

Amnesty International (2013). *Growing restrictions, tough conditions: The plight of those fleeing Syria to Jordan*. London: Amnesty International. Verkregen via: http://static.rasset.ie/documents/news/mde160032013en.pdf

CBS (Centraal Bureau voor de Statistiek) (2016), *Van opvang naar integratie: cohortstudie van recente asielmigranten.* www.cbs.nl/-/media/_pdf/2017/25/van%20opvang%20naar%20integratie_incl%20erratum.pdf

Converso, S., Bron, F. (ND). *Twenty-four Hours at the Grandhotel Cosmopolis in Augsburg. Stories of Work, Migration, and Collectivity*. Verkregen via: http://www.on-curating.org/issue-30-reader/twenty-four-hours-at-the-grandhotel-cosmopolis-in-augsburg-stories-of-work-migration-and-collectivity.html

Engbersen, G., J. Dagevos, R. Jennissen, L. Bakker & A. Leerkens (2015), *Geen tijd te verliezen: van opvang naar integratie van asielmigranten*. WRR Policy Brief 4. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid (WRR), Sociaal en Cultureel Planbureau (SCP), Wetenschappelijk Onderzoeks- en Documentatie Centrum, Ministerie van Veiligheid & Justitie (WODC).

Geuijen, K. (2004). *De asielcontroverse: debatteren over mensenrechten en nationale belangen*. Amsterdam: Rozenberg Publishers

Heber, G., Adamczyk, M. , Kochs, S. (2011). *Konzept für eine soziale Skulptur in Augsburgs Herzen*. Augsburg: Projektbüro „Grandhotel“

Immigratie en Naturalisatie Dienst (2018) *Asieltrends*. Verkregen via: https://ind.nl/over-ind/cijfers-publicaties/paginas/asieltrends.aspx

Ministerie van Justitie en Veiligheid (2018). *Integrale Migratieagenda* (Kamerbrief 29-03-2018). Verkregen via: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/29/tk-integrale-migratieagenda

Oliver, C., Dekker, R., Geuijen, K. (2018). *Plan Einstein, the Utrecht Refugee Launch Pad: Evaluation Interim Report*. Verkregen via: https://www.compas.ox.ac.uk/wp-content/uploads/URLP-interim-report-JULY-2018.pdf

RIVM (2016). *Nationaal Veiligheidsprofiel 2016*. Verkregen via: https://www.rivm.nl/RIVM/Organisatie/Centra/Centrum_Veiligheid/Analistennetwerk_Nationale_Veiligheid/Nationaal_Veiligheidsprofiel_2016

Hoofdstuk 6

The Arab Center for the Advancement of Social Media (2018). 7amleh. Verkregen via: http://7amleh.org/2018/07/12/the-new-israeli-cyber-law-paving-the-way-for-unlawful-hacking-and-digital-rights-violations/

Adamsky, D. (2017). The Israeli Odyssey toward its National Cyber Security Strategy. *The Washington Quarterly*, 40(2): 113-127.

Calcalist (2018). Israeli Civil Groups Warn Against Potential for Abuse in Cybersecurity Bill. Verkregen via: https://www.calcalistech.com/ctech/articles/0,7340,L-3741002,00.html

Council on Foreign Relations (2018). A look at Israel's new draft cybersecurity law. Verkregen via: https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law
The Privacy Protection Authority (2017). Privacy Protection (Data Security) Regulations. Verkregen via: https://www.gov.il/en/departments/general/data_security_eng

Cyber Security Research Center (2018). Cyber Law Program. Verkregen via: https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill-–-preliminary-overview

CyberSpark (2018). Why CyberSpark? Verkregen via: http://cyberspark.org.il/wp-content/uploads/2017/03/Why-CyberSpark-24.pdf.
Daskal, E. (2017). The Israeli Digital Rights Movement's campaign for privacy. *Internet Policy Review*, 6(3): 1-19.

European Commission (2016). Adequacy of the protection of personal data in non-EU countries. Verkregen via: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Hermann, T., Heller, E., Cohen, C., Beéry, G., Lebel Y. (2016). *The Israeli Democracy Index 2016*. Verkregen via: https://en.idi.org.il/media/7811/democracy-index-2016-eng.pdf

Housen-Couriel, D. (2017). CCDCOE NATO – Cooperative Cyber Defence Centre of Excellence. Verkregen via: https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf

Kamerstukken II 2016/2017, 34 588, nr. 3 (MvT), p. 6-7.

Karniel, Y., Lavie-Dinur, A. (2012). "Privacy in new media in Israel: How social networks are helping to shape the perception of privacy in Israeli society", *Journal of Information, Communication and Ethics in Society*, jrg. 10, nr. 4 (2012), p. 294.

Ministery of Justice (2017). Online Privacy Law: Israel. Verkregen via: https://www.loc.gov/law/help/online-privacy-law/2017/israel.php

Munnichs, G., Kouw, M., Kool, L. (2017). Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid. Den Haag: Rathenau Instituut.

National Cyber Directorate (2017). *Israel National Cyber Security Strategy in brief*, state of Israel, Prime Minister's Office. Tel Aviv: Israel.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018). Cybersecuritybeeld Nederland. Verkregen via: www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2018/1/CSBN_2018.pdf

Rijksdienst voor Ondernemend Nederland (2015). Overview IA Netwerk. Verkregen via: https://www.thehaguesecuritydelta.com/media/com_hsd/report/38/document/Overview-Cyber-Security-april-2015-digitaal.pdf.

Solomon, S. (2017). Israel works on 'digital Iron Dome' for cyberdefense. Verkregen via: https://www.timesofisrael.com/israel-works-on-digital-iron-dome-for-cyberdefense/

Solomon, S. (2018). Why is Israel's new proposed cybersecurity law raising hackles? Verkregen via: https://www.timesofisrael.com/why-is-israels-new-proposed-cybersecurity-law-raising-hackles/

Start-up Nation Central (2018). Cybersecurity brief, *Israel: a Global Center for Cyber Security*. Verkregen via: https://www.startupnationcentral.org/sector/cybersecurity/

Tabansky, L., Ben Israel, I. (2015). *Cybersecurity in Israel*. eBook: SpringerBriefs in Cybersecurity.

World Economic Forum (2018). *The Global Risks Report 2018*. Verkregen via: https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready

Hoofdstuk 7

Ministerie Justitie en Veiligheid (2018a). Slottoespraak minister Grapperhaus t.b.v. Kickstart Nationale Cyber Security Agenda 2018. Den Haag, Babylon, 24 mei 2018 Verkregen via: https://www.rijksoverheid.nl/onderwerpen/cybercrime/documenten/toespraken/2018/05/24/slottoespraak-minister-grapperhaus-tbv-kickstart-nationale-cyber-security-agenda-2018.-den-haag-babylon-24-mei-2018

Ministerie van Justitie en Veiligheid (2018b) Grapperhaus sluit cybersecurity alliantie met bedrijven om Nederland digitaal veilig te maken. Verkregen via: https://www.rijksoverheid.nl/onderwerpen/cybercrime/nieuws/2018/05/24/grapperhaus-sluit-cybersecurity-alliantie-met-bedrijven-om-nederland-digitaal-veilig-te-maken

Munnichs, G, Kouw, M., Kool, L. (2017) Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid. Den Haag: Rathenau Instituut

Mutsaers, B. (2018) Weerbaar door samenwerking? Een vergelijkend onderzoek naar triple-helix samenwerking bij innovatie op het gebied van cybersecurity in Nederland en Israël, Masterscriptie Publiek Management, Universiteit Utrecht.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018). Cybersecuritybeeld Nederland. Verkregen via: https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf

NOS (2018). Extra geld voor aanpak cybercrime Verkregen via: https://nos.nl/artikel/2250003-extra-geld-voor-aanpak-cybercrime.html

Rathenau Instituut (2018). Digitale samenleving. Verkregen via: https://www.rathenau.nl/nl/digitale-samenleving/overheid-en-bedrijven-onvoldoende-beschermd-tegen-cyberdreigingen

Rijksoverheid (2018). Over het Digital Trust Center. Verkregen via: https://www.digitaltrustcenter.nl/over-het-digital-trust-center

Rijksinstituut voor Volksgezondheid en Milieu (2016). Nationaal Veiligheidsprofiel 2016. Verkregen via: https://www.nctv.nl/binaries/Nationaal%20Veiligheidsprofiel%202016_tcm31-232083.pdf