Universiteit Utrecht

USBO
advies

Op weg naar een Weerbare Open Samenleving

Bouwstenen voor een toekomstvisie

definitief

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.

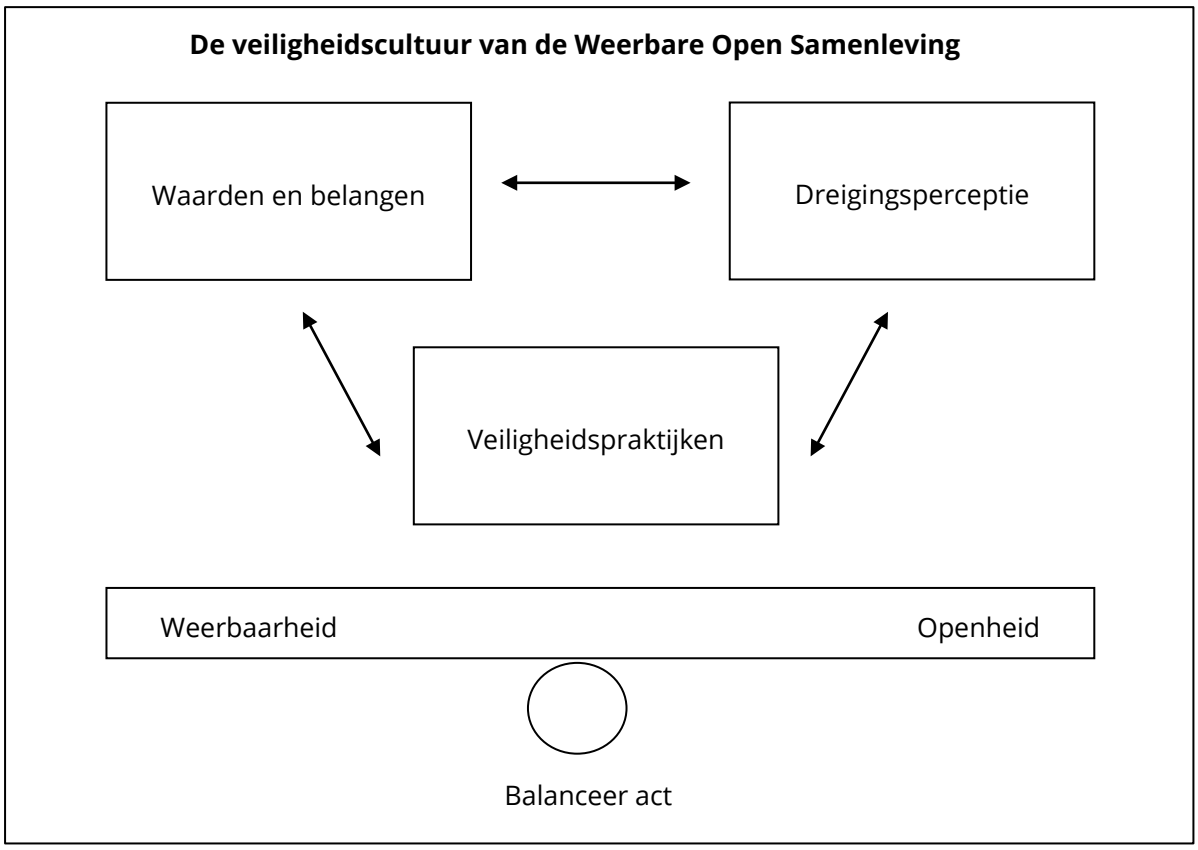
Analysekader

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.