

Rapportage WP 1120

Veiligheid en grondrechten in Secure Haven

Mr. dr. B.W. Schermer

Prof. dr. A.H.J. Schmidt

Dr. L. Mommers

Management-samenvatting deel 1

Risico's (criminaliteit, terrorisme) die ontstaan door bewust menselijk handelen zijn inherent aan het leven in een complexe en globale samenleving. Deze risico's kunnen (deels) beperkt en beheerst worden door het nemen van veiligheidsmaatregelen. Echter, onder omstandigheden kunnen veiligheidsmaatregelen op gespannen voet staan met de grondrechten van individuen. In deze rapportage is een onderzoek gedaan naar de verhouding tussen grondrechten en veiligheid binnen Secure Haven. In een Secure Haven dienen veiligheid en respect voor grondrechten hand in hand te gaan. De probleemstelling van deze rapportage luidt dan ook:

Hoe kunnen veiligheid en respect voor grondrechten tegelijkertijd optimaal gewaarborgd worden binnen Secure Haven?

In hoofdstuk 1 tot en met 3 zal een algemene inleiding worden gegeven, de probleemstelling uiteen worden gezet en in gegaan op de veiligheidsrisico's die binnen Secure Haven geadresseerd (moeten) worden. In de hoofdstukken 4, 5 en 6 is het juridisch kader voor de bescherming van grondrechten uiteengezet. Uit deze uiteenzetting blijkt dat het recht op privacy een voorname plaats inneemt in de discussie over grondrechten en veiligheid. Een belangrijke reden hiervoor is dat het recht op privacy gebruikt kan worden om gedrag en informatie af te schermen van derden. Als zodanig is privacy niet alleen een onmisbare voorwaarde voor de individuele autonomie en menselijke waardigheid, maar ook een middel om diverse andere grondrechten te beschermen.

In hoofdstuk 7 wordt ingegaan op veiligheid en opsporing. Grondrechten, waaronder het recht op privacy, zijn niet absoluut, en ze kunnen dus worden beperkt. Het waarborgen van de veiligheid en openbare orde is een mogelijke grond voor de (tijdelijke) beperking van grondrechten. Aan een dergelijke beperking moet echter wel een strenge toetsing vooraf gaan om in te schatten of de inperking van het grondrecht effectief, legitiem en proportioneel is. Ook moet getoetst worden of geen minder ingrijpende methoden denkbaar zijn om de veiligheid te waarborgen.

In hoofdstuk 8 worden technologische trends beschreven die richting 2017 met name van invloed zijn op het veiligheidsdomein. In hoofdstuk 9 worden mede aan de hand van de conclusies uit hoofdstuk 8 de mogelijke risico's voor de grondrechten van burgers bij de toepassing van veiligheidsmaatregelen in hun onderlinge samenhang besproken. Mogelijke risico's hebben betrekking op de machtsverhouding tussen burger en overheid, maatschappelijke schifting, het verlies aan sociale cohesie en verhoogde kans op vals-positieven.

In hoofdstuk 10 wordt vervolgens teruggegrepen op het concept privacy en gekeken wat het belang van privacy is bij de bescherming van grondrechten en het voorkomen van de risico's zoals gesignaleerd in hoofdstuk 9. In hoofdstuk 11 zijn de belangrijkste toetsingscriteria voor de toepassing van veiligheidsmaatregelen binnen Secure Haven gegeven. Een eerste toetsingscriterium dat geschetst is, is de effectiviteit van een maatregel. Wanneer een veiligheidsmaatregel niet effectief is, omdat het niet het beoogde doel van het vergroten van de veiligheid kan bewerkstelligen, of er maatregelen zijn die beter en/of meer kosteneffectief zijn, is dit een belangrijke indicatie om de maatregel niet in te voeren. Een dergelijke effectiviteitstoetsing staat zelfs nog los van de vraag of er überhaupt sprake is van een inbreuk op de grondrechten van burgers.

Wanneer een veiligheidsmaatregel effectief is (of kan zijn), is de volgende stap in de toetsing het bekijken in hoeverre deze veiligheidsmaatregel inbreuk maakt op de grondrechten van burgers. Het verdient nadruk om te stellen dat veiligheid en individuele grondrechten niet per definitie tegenover elkaar staan. Het zijn beide waarden die gemaximaliseerd dienen te worden binnen onze maatschappij. Wanneer er geen andere mogelijkheid bestaat om veiligheid te garanderen dan een inbreuk op grondrechten, dient gekeken te worden in hoeverre voor een vergroting van de veiligheid een inbreuk op de grondrechten van een individu of groep gerechtvaardigd is. Een dergelijke toetsing is vooraf vaak moeilijk te maken.

Het toetsingskader zoals beschreven in hoofdstuk 11 en een bewustzijn rondom de mogelijke risico's die veiligheidsmaatregelen zelf voor onze democratie en rechtsstaat kunnen vormen (onder andere verschuiving van de machtsbalans, panoptische gevoelens, het verlies van sociale cohesie en het risico op vals-positieven), vormen belangrijke aanknopingspunten voor een weloverwogen beslissing. Ook de blijvende democratische

legitimatie via transparantie, een goed systeem van ‘checks and balances’, periodieke evaluaties en waar mogelijk een limitering op de duur van een maatregel en/of bevoegdheid is van groot belang bij het beoordelen of een maatregel al dan niet acceptabel is.

Belangrijke voorwaarde voor de invoering van veiligheidsmaatregelen die inbreuk maakt (of kan maken) op de grondrechten van het individu is dat de inbreuk gebaseerd is op een wettelijke grondslag. Hierbij kan opgemerkt worden dat bij de invoering van veiligheidsmaatregelen de zelfstandige bevoegdheid van de gemeente Den Haag veelal beperkt is. Dit geldt met name voor het uitbreiden van de bevoegdheden van opsporingsambtenaren.

Met het oog op de doelstellingen van Secure Haven (een veilige, prettige leefomgeving) is het ook van belang om te kijken in hoeverre de invoering van veiligheidsmaatregelen ongewenste negatieve effecten kan hebben op de leefbaarheid binnen Secure Haven. Voor de leefbaarheid van Secure Haven is immers niet alleen veiligheid (of een gevoel van veiligheid) van belang, maar speelt ook respect voor de grondrechten van het individu een belangrijke rol. Burgers kunnen een negatief gevoel krijgen over Secure Haven wanneer zij voelen dat er een te grote inmenging is in hun persoonlijke levenssfeer. Ook de frequentie van ‘vals positieven’ speelt hierbij een rol.

We kunnen concluderen dat voor een Secure Haven het maximaliseren van veiligheid en het respect voor grondrechten hand in hand dienen te gaan. Daar waar het ene belang aan het andere in de weg staat dient een zeer zorgvuldige afweging te worden gemaakt.

Inhoudsopgave deel 1

1	INLEIDING	6
2	PROBLEEMSTELLING	6
2.1	VRAAGSTELLING	7
3	VEILIGHEIDSRISICO'S	7
4	ALGEMEEN JURIDISCH KADER	8
4.1	GRONDRECHTEN.....	8
4.2	INTERNATIONALE VERDRAGEN	8
4.2.1	<i>Universele Verklaring van de Rechten van de Mens (1948)</i>	8
4.2.2	<i>Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (1976)</i>	8
4.2.3	<i>Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (1950)</i>	8
4.3	NEDERLANDSE SITUATIE	9
4.3.1	<i>Grondwet</i>	9
4.3.2	<i>Wet- en regelgeving</i>	9
5	GRONDRECHTEN IN EEN SECURE HAVEN	10
5.1	HET RECHT OP GELIJKE BEHANDELING (ARTIKEL 1 GRONDWET)	10
5.2	VRIJHEID VAN GODSDIENST EN LEVENSOVERTUIGING (ARTIKEL 6 GRONDWET)	10
5.3	VRIJHEID VAN MENINGSUITING (ARTIKEL 7 GRONDWET).....	10
5.4	HET RECHT OP VRIJHEID VAN VERGADERING EN BETOGING (ARTIKEL 9 GRONDWET).....	11
5.5	HET RECHT OP BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (ARTIKEL 10 T/M 13 GRONDWET)	11
5.6	HET RECHT OP EEN EERLIJK PROCES (ARTIKEL 17 T/M 18 GRONDWET / ARTIKEL 6 EVRM).....	11
6	PRIVACY IN EEN SECURE HAVEN	12
6.1	DEFINITIE	12
6.2	PRIVACY EN PERSOONSgegevens	12
6.2.1	<i>De zorgvuldige verwerking van persoonsgegevens</i>	13
6.3	PRIVACY EN PUBLIEKE RUIMTE	13
6.3.1	<i>De 'reasonable expectation of privacy'</i>	14
6.3.2	<i>Informationele privacy en de publieke ruimte</i>	14
7	VEILIGHEID EN OPSPORING BINNEN SECURE HAVEN	16
7.1	PREVENTIE.....	16
7.1.1	<i>De zelfstandigheid van de Internationale Zone</i>	17
7.1.2	<i>Relevantie voor Secure Haven</i>	17
7.2	OPSPORING	17
7.2.1	<i>Reactieve opsporing</i>	18
7.2.2	<i>Pro-actieve opsporing</i>	18
7.2.3	<i>Relevantie voor Secure Haven</i>	18
7.3	GEGEENSVERWERKINGEN BINNEN SECURE HAVEN	18
8	TECHNOLOGISCHE ONTWIKKELINGEN	20
8.1	ALOMTEGENWOORDIGHEID ICT	20
8.2	VERBETERDE INFORMATIEHUISHOUDING	20
8.3	VEILIGHEIDSMaatregelen Richting 2017	21
8.3.1	<i>Monitoring</i>	21
8.3.2	<i>Intelligence led policing</i>	22
8.3.3	<i>Datamining en profiling</i>	22
8.3.4	<i>Real time monitoring en sharing</i>	22
8.4	TUSSENCONCLUSIE.....	22
9	RISICO'S VOORTVLOEIEND UIT VEILIGHEIDSMaatregelen	23
9.1	PREVENTIEF: HET PANOPTICON.....	23

9.1.1	<i>Verschuiving van de machtsbalans</i>	24
9.1.2	<i>Sociale cohesie en discriminatie</i>	24
9.1.3	<i>Transparantie en democratische borging</i>	24
9.2	OPSPORING: REACTIEF.....	24
9.2.1	<i>Inmenging in de persoonlijke levenssfeer</i>	25
9.2.2	<i>Function- en mission creep</i>	25
9.3	OPSPORING: PRO-ACTIEF.....	25
9.3.1	<i>Risicojustitie</i>	25
10	PRIVACY, AUTONOMIE EN GRONDRECHTEN	27
11	GRONDRECHTEN EN VEILIGHEID	27
11.1	EFFECTIVITEIT VEILIGHEIDSMATREGELEN.....	28
11.2	EISEN VANUIT HET RECHT.....	29
11.2.1	<i>Bij de wet voorzien</i>	30
11.2.2	<i>Noodzakelijk in een democratische samenleving</i>	30
11.3	TOETSINGSCRITERIA VERHOUDING VEILIGHEID EN GRONDRECHTEN.....	30
11.3.1	<i>Beïnvloeding bestaande machtsverhoudingen</i>	30
11.3.2	<i>Beïnvloeding gedrag burgers</i>	30
11.3.3	<i>Mogelijkheden tot misbruik</i>	31
11.3.4	<i>Checks and balances</i>	31
11.3.5	<i>Transparantie</i>	31
11.3.6	<i>Informationele zelfbeschikking</i>	31
12	OPLOSSINGSRICHTINGEN	33
12.1	DEMOCRATISCHE LEGITIMATIE EN BORGING.....	33
12.1.1	<i>Burgerparticipatie</i>	33
12.2	PERIODIEKE TOETSING.....	33
12.3	LIMITERING DUUR VEILIGHEIDSMATREGELEN.....	33
12.4	VOORKOMEN SYSTEEMDWANG.....	33
12.5	PRIVACY BY DESIGN.....	34
12.5.1	<i>Minimalisatie en anonimisering</i>	34
13	CONCLUSIE	34
14	AANBEVELINGEN	36
15	VERKORTE BIBLIOGRAFIE	37
16	APPENDIX	39
16.1	SCENARIO'S.....	39
16.1.1	<i>Casus Secure Convention Center district</i>	39
16.1.2	<i>Casus Congresgebied</i>	40
16.1.3	<i>Casus Secure City Manager</i>	41

1 Inleiding

Het Secure Haven programma heeft tot doel om van Den Haag, meer specifiek de Internationale Zone, een veilige(re) en prettige(re) leefomgeving te maken. Veiligheid (in de zin van 'security') is in deze context het afwezig zijn van situaties waarin zich bewust gecreëerde risico's voor personen, goederen en gebouwen kunnen voordoen. Het gaat hierbij om een scala aan risico's variërend van zakkenrollen tot gecoördineerde vormen van (internationaal) terrorisme. Om veiligheid te creëren of te vergroten dienen risicofactoren geminimaliseerd te worden. Door het introduceren van veiligheidsmaatregelen kunnen risico's geminimaliseerd worden, waardoor veiligheid toeneemt.

Echter, veiligheidsmaatregelen kunnen onder omstandigheden op gespannen voet staan met grondrechten, zoals het recht op gelijke behandeling (artikel 1 Grondwet), het recht op vrijheid van godsdienst/levensovertuiging (artikel 6 Grondwet), het recht op vrijheid van meningsuiting (artikel 7 Grondwet), het recht op vrijheid van vereniging (artikel 8 Grondwet), het recht op vrijheid van vergadering en betoging (artikel 9 Grondwet) en het recht op privacy (artikel 10 tot en met 13 Grondwet). In werkpakket 1120 van het Secure Haven project wordt bekeken in hoeverre maatregelen ter bevordering van de veiligheid zich verhouden tot de verschillende grondrechten zoals vastgelegd in de Nederlandse Grondwet en internationale verdragen, waaronder het EVRM.

2 Probleemstelling

Wil een mens zich vrij voelen en zichzelf kunnen ontplooiën, dan heeft hij een zekere mate van veiligheid nodig. Veiligheid, the *freedom from fear*, werd daarom door Roosevelt in zijn beroemde speech voor het Amerikaanse Congres betiteld als één van de vier fundamentele vrijheden.¹ Het is de taak van de staat om haar soevereiniteit te verdedigen en de veiligheid van haar burgers te garanderen. Dit betekent dat de staat maatregelen moet nemen om externe en interne bedreigingen van de veiligheid te adresseren. Voor Secure Haven betekent dit dat er maatregelen genomen dienen te worden die de openbare orde en de veiligheid van de bewoners en bezoekers van Secure Haven vergroten.

Een ander cruciaal onderdeel van de vrijheid van de mens vormt diens persoonlijke autonomie, oftewel het gevrijwaard blijven van externe beïnvloeding.² Deze persoonlijke autonomie wordt gewaarborgd en expliciet gemaakt via grondrechten. Naast veiligheid vormen de grondrechten van de burger dus noodzakelijke voorwaarden voor diens vrijheid.

Voor het Secure Haven project betekent dit dat er een leefomgeving gecreëerd moet worden die veilig is en waarin de grondrechten van burgers en bezoekers gerespecteerd worden en zo min mogelijk worden gehinderd in hun doen en laten. Tussen het garanderen van veiligheid en autonomie bestaat echter een spanningsveld. Om de openbare orde en de veiligheid van de burger te garanderen, moet onder omstandigheden inbreuk worden gemaakt op de grondrechten van burgers.³ De uitdaging voor het Secure Haven project ligt in het waarborgen van deze beide belangen.

Aldus kunnen we het volgende constateren:

- 1) Respect voor grondrechten en het garanderen van veiligheid zijn waarden die beide gemaximaliseerd dienen te worden binnen Secure Haven.
- 2) Veiligheid en grondrechten kunnen op gespannen voet met elkaar staan binnen Secure Haven, omdat voor het garanderen van veiligheid mogelijk afbreuk moet worden gedaan aan de autonomie van het individu.

¹ Roosevelt, F. D. R. (1941), *Annual Address to Congress 'the Four Freedoms'*, 6 januari 1941

² Zie voor een uitgebreide uitleg van dit idee het essay *Two Concepts of Liberty* van Isaiah Berlin (1958)

³ De toepassing van opsporingsbevoegdheden en dwangmiddelen door de politie is goed voorbeeld waar individuele grondrechten moeten wijken voor het belang van de veiligheid en openbare orde.

Op basis van deze twee constatering kunnen we voor deze rapportage de volgende probleemstelling formuleren:

Hoe kunnen veiligheid en respect voor grondrechten tegelijkertijd optimaal gewaarborgd worden binnen Secure Haven?

2.1 Vraagstelling

Bij deze probleemstelling kunnen de volgende (rechts)vragen worden gesteld:

- 1) Wat is het juridisch kader voor de bescherming van grondrechten?
- 2) Welke risico's kunnen er ontstaan voor de grondrechten van burgers bij de toepassing van veiligheidsmaatregelen?
- 3) Wat is het (juridische) toetsingskader voor de bescherming van grondrechten?
- 4) Welke oplossingsrichtingen zijn er om veiligheid en bescherming van grondrechten met elkaar te verenigen?

In deze rapportage zal een aanzet worden gedaan voor een toetsingskader op basis waaraan beleidsmakers en beslissers de invoering van veiligheidsmaatregelen binnen Secure Haven kunnen toetsen. Een toetsing van de effectiviteit en legitimiteit van concrete veiligheidsmaatregelen valt overigens buiten de scope van deze rapportage. In deze rapportage zal een algemeen (toetsings)kader worden geschetst. Via de techniek van het 'legal requirements engineering' zal dit algemene toetsingskader verder verscherpt worden. Deze verscherping is vastgelegd in een aparte rapportage. Voor de volledigheid zijn de in deze tweede rapportage gebruikte scenario's ook als appendix bij deze rapportage opgenomen.

3 Veiligheidsrisico's

Binnen Secure Haven willen we een convergentie van subjectieve en objectieve veiligheid bevorderen. Verschillende veiligheidsrisico's worden met regelmaat door media en politiek voor het voetlicht gebracht. Het gaat om heel diverse risico's, zoals terroristische aanslagen, criminaliteit, natuur- en milieurampen en rampen veroorzaakt door menselijk handelen of nalaten. Doorgaans leidt die aandacht tot een 'opwaartse druk' op de overheid: de druk om te handelen en risico's te reduceren.

Wanneer we kijken naar bedreigingen voor de veiligheid die zich kunnen voordoen dan kunnen we deze bedreigingen naar oorzaak onderscheiden:

- 1) Bedreigingen zonder menselijke component (bijvoorbeeld natuurrampen)
- 2) Bedreigingen voortvloeiend uit onbewust menselijk handelen (ongelukken)
- 3) Bedreigingen die voortvloeien uit bewust menselijk handelen (bijvoorbeeld criminaliteit en terrorisme)

Binnen het Secure Haven concept zijn er verschillende typen maatregelen zijn die gericht zijn op het minimaliseren van risico's uit deze drie categorieën. Met name maatregelen uit de derde categorie kunnen op gespannen voet staan met de grondrechten van de burger, omdat de overheid actief moet ingrijpen in de persoonlijke levenssfeer van haar burgers. Wanneer wij het in deze rapportage hebben over veiligheidsmaatregelen dan doelen wij op veiligheidsmaatregelen die primair tot doel hebben om risico's uit deze derde categorie te verkleinen.

4 Algemeen juridisch kader

In dit werkpakket (WP 1120) wordt het juridisch kader voor de bescherming van grondrechten getoetst aan het ‘veiligheidsconcept’ dat binnen het Secure Haven project ontwikkeld wordt. Hiertoe zal allereerst een overzicht worden gegeven van het relevante juridische kader.

4.1 Grondrechten

De grenzen van hetgeen de staat is toegestaan bij de inmenging in het leven van haar onderdanen (en onderdanen van andere staten) worden gesteld door internationale verdragen en de Grondwet.

Een rechtsstaat karakteriseert zich mede door de vastlegging en bescherming van grondrechten. Er kan hierbij onderscheid worden gemaakt tussen ‘klassieke’ en ‘sociale’ grondrechten. Klassieke grondrechten zijn rechten van burgers die door de overheid gerespecteerd dienen te worden en die de overheid over het algemeen beperken in haar machtsuitoefening richting burgers. Klassieke grondrechten beschermen de burgers dus tegen de overheid, en limiteren de inmenging van overheidswegen in het persoonlijke leven. Het gaat dan bijvoorbeeld om de vrijheid van meningsuiting (artikel 7 Grondwet) en de eerbiediging van de persoonlijke levenssfeer (artikel 10 Grondwet).

Sociale grondrechten zijn rechten van burgers waar een inspanning van de overheid wordt vereist om deze rechten gestalte te geven. Het gaat dan bijvoorbeeld op het recht op werkgelegenheid (artikel 19 Grondwet) en het recht op onderwijs (artikel 23 Grondwet).

Met het oog op het onderwerp van deze rapportage zullen wij ons met name richten op de bespreking van de klassieke grondrechten en hun plek binnen het Secure Haven concept, omdat hoofdzakelijk deze rechten bij het Secure Haven concept in het geding kunnen komen.

4.2 Internationale verdragen

De klassieke grondrechten zijn vastgelegd in diverse internationale verdragen. Hieronder zal een kort overzicht worden gegeven van de belangrijkste verdragen.

4.2.1 *Universele Verklaring van de Rechten van de Mens (1948)*

Met de gruwelen van de Tweede Wereldoorlog nog vers in het geheugen werd op 10 december 1948 de Universele Verklaring van de Rechten van de Mens aangenomen door de Verenigde Naties. De Universele Verklaring bevat onder andere het grondrecht op gelijke behandeling (artikel 1), eerbiediging van de persoonlijke levenssfeer (privacy) (artikel 12) en vrijheid van meningsuiting (artikel 19). Hoewel de Universele Verklaring bij de proclamatie geen bindende kracht had voor de deelnemende staten, heeft het verdrag door de implementatie in het nationale recht van de deelnemende staten *de facto* grote zeggingskracht (Rotenberg, 2003, p. 316).

4.2.2 *Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (1976)*

Gegeven het feit dat Universele Verklaring *de jure* niet-bindend is, werd in 1966 het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) aangenomen. Het verdrag trad in 1976 werking na ratificatie door 35 landen. Het IVBPR is in tegenstelling tot de Universele Verklaring wél bindend voor de deelnemers aan het verdrag. Handhaving van het verdrag vindt voornamelijk plaats via het VN-comité voor de mensenrechten. Deelnemende staten zijn verplicht aan het Comité te rapporteren over de mensenrechtensituatie in hun land.

4.2.3 *Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (1950)*

In 1950 werd het Europese Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) aangenomen door de Raad van Europa. Dit verdrag, waar Nederland ook partij bij is, is van groot belang, omdat het als verdrag niet alleen prevaleert boven het nationale recht van Nederland, maar ook een ‘eigen’ gerechtelijke instantie kent, te weten het Europese Hof voor de Rechten van de Mens (EHRM). Daar kunnen burgers van aan het verdrag deelnemende lidstaten hun beklag doen. Met het oog op het Secure Haven programma zijn de volgende rechten specifiek van belang: 1) het recht op vrijheid en veiligheid (arti-

kel 5 EVRM), het recht op een eerlijk proces (artikel 6 EVRM), eerbiediging van de persoonlijke levenssfeer (artikel 8 EVRM), vrijheid van geweten en godsdienst (artikel 9 EVRM), vrijheid van meningsuiting (artikel 10 EVRM), vrijheid van vergadering en vereniging (artikel 11 EVRM) en het recht op gelijke behandeling (artikel 14 EVRM).

4.3 Nederlandse situatie

Nederland is partij bij alle bovengenoemde verdragen. Daarnaast blijft uiteraard de Nederlandse Grondwet een belangrijke rechtsbron.

4.3.1 Grondwet

In onze Grondwet staan diverse klassieke grondrechten die met het oog op veiligheidsmaatregelen binnen het Secure Haven concept onder druk kunnen komen te staan. Het gaat hoofdzakelijk om de volgende klassieke grondrechten: 1) het recht op gelijke behandeling (artikel 1 Grondwet), 2) het recht op vrijheid van godsdienst/levensovertuiging (artikel 6 Grondwet), 3) het recht op vrijheid van meningsuiting (artikel 7 Grondwet), 4) het recht op vrijheid van vereniging (artikel 8 Grondwet), 5) het recht op vrijheid van vergadering en betoging (artikel 9 Grondwet) en 6) het recht op privacy (artikel 10 tot en met 13 Grondwet).

Het is belangrijk te vermelden dat de grondrechten waarop een individu zich kan beroepen niet absoluut zijn. Met andere woorden, het is onder omstandigheden mogelijk om de werking van grondrechten in te perken. Redenen om grondrechten te beperken zijn bijvoorbeeld de schending van de grondrechten van een ander, of de gerechtvaardigde belangen van de samenleving als geheel. Veiligheid is een van deze gerechtvaardigde belangen en *kan* dus prevaleren boven de grondrechten van een individu. De Grondwet zelf geeft aan op welke gebieden uitzonderingen kunnen worden gemaakt, en op welke wijze dat dient te gebeuren.

4.3.2 Wet- en regelgeving

De bepalingen uit de Grondwet krijgen nader gestalte in wetgeving in formele zin, en in regelgeving die op deze wetgeving gebaseerd is. Zo vinden we de regels omtrent de bescherming van de persoonlijke levenssfeer (artikel 10 t/m 13 Grondwet) onder andere terug in het Wetboek van Strafvordering, de Wet Politiegegevens, de Wet bescherming persoonsgegevens en de Telecommunicatiewet, en gedelegeerde regelgeving.

5 Grondrechten in een Secure Haven

Hoewel veiligheid van essentieel belang is voor de vrijheid en het geluk van de burgers van een staat, kan een te grote invloed van de staat op het leven van de burger ook een negatief gevoel opwekken bij de burger, en diens grondrechten aantasten. Het is dus van belang met het oog op de doelstellingen van Secure Haven om zowel de veiligheid als het respect voor de grondrechten van de burgers en bezoekers van Den Haag te maximaliseren.

Gegeven de potentiële frictie tussen veiligheidsmaatregelen en grondrechten is het van belang om de grondrechten die in het kader van Secure Haven in het geding kunnen komen nader te bespreken. Na deze bespreking kan vervolgens een toetsingskader worden geschapen voor een verantwoorde toepassing van veiligheidsmaatregelen binnen Secure Haven.

5.1 Het recht op gelijke behandeling (artikel 1 Grondwet)

Het recht op gelijke behandeling, ook wel gekarakteriseerd als het verbod op discriminatie, verbiedt het maken van onderscheid bij behandeling in gelijke gevallen tussen personen op basis van bijvoorbeeld ras, godsdienst, geslacht of politieke gezindheid. Bij veiligheidsmaatregelen bestaat altijd het risico dat deze bewust of onbewust onevenredig vaak worden toegepast op een bepaalde groep, omdat deze groep op basis van raciale, godsdienstige, politieke of andere gronden worden gezien als een 'risicogroep'. Dit heeft tot gevolg dat deze (vermeende) risicogroepen (bijvoorbeeld orthodoxe moslims of Antilliaanse jongeren) vaker het onderwerp zijn van veiligheids- en controlemaatregelen. Deze directe discriminatie is bij wet verboden. Bij veiligheidsmaatregelen kan er ook sprake zijn van indirecte discriminatie. Een voorbeeld is het verbod op het dragen van een boerka als men een publieke ruimte betreedt. Hoewel indirecte discriminatie onder bepaalde omstandigheden toegestaan kan zijn als dit noodzakelijk en redelijk is, moet bij het creëren van veiligheidsmaatregelen ook tegen deze vorm van discriminatie gewaakt worden.

5.2 Vrijheid van godsdienst en levensovertuiging (artikel 6 Grondwet)

In het verlengde van hetgeen besproken bij het recht op gelijke behandeling, kan de vrijheid van godsdienst en levensovertuiging in het gedrang komen bij de toepassing van veiligheidsmaatregelen. Een sprekend voorbeeld is wederom het 'boerka-verbod'.⁴ Dit verbod dat (deels) het vergroten van de (nationale) veiligheid tot doel heeft staat op gespannen voet met de vrijheid van moslimvrouwen om hun geloof te belijden.⁵

5.3 Vrijheid van meningsuiting (artikel 7 Grondwet)

De vrijheid van meningsuiting is één van de belangrijkste verworvenheden van onze democratische rechtsstaat. Hoewel de vrijheid van meningsuiting niet absoluut is, staat het een ieder in Nederland in principe vrij zijn mening te uiten, ook als deze mening anderen onwelgevallig is. Dit betekent dat het burgers ook vrij staat politiek en overheid (het 'gezag') met woord en daad te bekritisieren.

Sommige kritiek kan door de machthebbers als kwetsend, opruiend of zelfs staatsgevaarlijk worden ervaren. In dergelijke gevallen zal de vrijheid van meningsuiting beperkt worden en kunnen er (strafrechtelijke) sancties volgen tegen degenen die hun mening hebben geuit. De dreiging van dergelijke sancties kan tot gevolg hebben dat mensen terughoudender worden in het uiten van hun mening. Tot op heden heeft de mogelijkheid om anoniem een mening te uiten er voor gezorgd dat mensen niet terughoudend hoeven te zijn in het uiten van hun mening. Wanneer echter door toepassing van veiligheidsmaatregelen de anonimiteit van degene die zijn mening uit wordt opgeheven (en deze dus te vervolgen is), kan dat een bevriezende werking hebben op

⁴ Kamerstukken 2007-2008, 31 108, nrs. 1-7

⁵ Zie: http://www.ivir.nl/publicaties/dommering/NRC_boerkaverbod.html

de vrijheid van meningsuiting.⁶ Een dergelijke ontwikkeling is schadelijk voor het democratisch proces en de rechtsstaat.

5.4 Het recht op vrijheid van vergadering en betoging (artikel 9 Grondwet)

In het verlengde van de vrijheid van meningsuiting ligt het recht op vrijheid van vergadering en betoging. Wanneer het door veiligheidsmaatregelen moeilijker wordt om in relatieve anonimiteit/afzondering gelijkgestemden te ontmoeten en samen met hen een mening te vormen, dan is dit potentieel schadelijk voor het democratisch proces. Ook het gezamenlijk uiten van een mening door middel van een betoging (demonstraties en dergelijke) kan door veiligheidsmaatregelen worden ingeperkt. Uit angst voor negatieve gevolgen van het geassocieerd worden met een bepaalde betoging of mening, kunnen mensen terughoudender worden in het uiten van hun mening. Een voorbeeld is het filmen van demonstranten door de overheid en het vragen naar hun identiteit. Een mogelijk gevolg van deze praktijken is dat mensen niet (meer) meedoen met betogingen.

5.5 Het recht op bescherming van de persoonlijke levenssfeer (artikel 10 t/m 13 Grondwet)

Het recht op bescherming van de persoonlijke levenssfeer, in de volksmond beter bekend als het recht op privacy, beschermt de burger tegen ongewenste inmenging van derden (meer specifiek de overheid) in diens privéaangelegenheden. Wanneer we kijken naar de toepassing van veiligheidsmaatregelen dan valt te constateren dat het grondrecht op bescherming van de persoonlijke levenssfeer direct onder druk staat van deze maatregelen. Het recht op privacy speelt dan ook een dusdanig belangrijke rol binnen de discussie rondom veiligheid en het waarborgen van grondrechten, dat er apart aandacht aan zal worden besteed in het volgende hoofdstuk.

5.6 Het recht op een eerlijk proces (artikel 17 t/m 18 Grondwet / artikel 6 EVRM)

In de Nederlandse grondwet is het recht op een eerlijk proces primair vastgelegd in artikel 17 en 18 Grondwet. Het EVRM geeft in artikel 6 een volledige opsomming van de onderdelen van een eerlijk proces. Het gaat hierbij om toegang tot de rechter, bijstand van een advocaat enzovoorts. In samenhang met het legaliteitsbeginsel, dat bepaalt dat er geen straf is zonder voorafgaande strafbepaling, waarborgen deze grondrechten mede de rechtspositie van de burger. Het recht op een eerlijk proces kan in het geding komen wanneer onduidelijk is op welke wijze bewijs (bijvoorbeeld via veiligheidsmaatregelen) is vergaard en of dit toelaatbaar is in een eventueel strafproces.

⁶ Hierbij dient wel de kanttekening worden gemaakt dat het volledig anoniem uiten van meningen via bijvoorbeeld internetfora ook negatieve effecten kan hebben. Dergelijke gelegenheden bieden immers ook de mogelijkheid tot het ongestraft doen van beledigende en discriminatoire uitingen.

6 Privacy in een Secure Haven

In het debat over veiligheid komt het recht op privacy al snel ter sprake. Voorstanders van strikte(re) veiligheidsmaatregelen voeren het recht op privacy veelal aan als een struikelblok bij de bescherming van de (nationale) veiligheid, terwijl de tegenstanders van strikte(re) veiligheidsmaatregelen aanvoeren dat door de veiligheidsdrang van de overheid het recht op privacy steeds verder afkalft. Omdat in het debat rondom veiligheid en grondrechten nagenoeg altijd het recht op privacy de boventoon voert, zal in dit hoofdstuk extra aandacht worden besteed aan het recht op privacy. Het is echter van belang om in het achterhoofd te houden dat het recht op privacy vaak wordt gebruikt als middel om andere grondrechten te beschermen.⁷

6.1 Definitie

Een eenduidige definitie van het begrip privacy is moeilijk tot niet te geven. Dit komt hoofdzakelijk door het feit dat het begrip privacy slechts vorm krijgt door verwijzing naar een complex geheel van sociale, culturele, politieke, juridische en filosofische factoren waarvan het afhankelijk is (Gutwirth, 1998). Het recht op privacy beschermt een nauw omliggende, maar relatief onschendbare persoonlijke levenssfeer tegen bemoeienis van buitenstaanders (Blok, 2002). In dit kader kan het recht op privacy onderverdeeld worden in een aantal concepties (wat tracht men met het recht op privacy te bewerkstelligen) en een aantal dimensies (waarop is het recht op privacy van toepassing) (Schermer, 2007, p. 71). Tot de concepties van het recht op privacy behoren onder andere: het beschermen van de persoonlijke autonomie, het afsluiten voor invloeden van buitenaf en het mogelijk maken van sociale interactie. Tot de dimensies van privacy behoren onder andere: het lichaam, het huis, de communicatie en het familieleven (Nieuwenhuis, 2001, p. 31).

6.2 Privacy en persoonsgegevens

Technologie heeft altijd een grote invloed gehad op de ontwikkeling van het recht op privacy. Je zou zelfs kunnen stellen dat een technologische ontwikkeling (die van de fotocamera) van doorslaggevende betekenis is geweest bij het formuleren van het recht op privacy. Het recht op privacy werd voor het eerst genoemd in een publicatie van Warren en Brandeis (1890) waarin zij zich kritisch uitlieten over de Amerikaanse roddelpers die met behulp van fotocamera's privé aangelegenheden vastlegden.

Met de komst van het computertijdperk werd het steeds beter mogelijk om gegevens op te slaan, te verwerken en door te sturen. Dit gold uiteraard ook voor informatie over personen (zogenoemde persoonsgegevens). Door de ontwikkeling van de computer ontstond er een nieuwe richting in het privacy denken, die van de 'informatieprivacy' (Westin, 1967).

De informatieprivacy gaat er vanuit dat het individu zelf moet kunnen bepalen welke informatie over hem beschikbaar is. Of zoals Westin (1967) het beschrijft:

“The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated.”

Voor de bescherming van de informatieprivacy is de bescherming van persoonsgegevens van essentieel belang. Het denken over de informatieprivacy heeft uiteindelijk tot de wettelijke bescherming van persoonsgegevens geleid. Deze bescherming krijgt in Nederland onder andere gestalte via de Wet bescherming persoonsgegevens en de Wet politiegegevens.

Met het oog op het Secure Haven concept is het idee van informatieprivacy van belang omdat vermoedelijk veel van de voorgestelde veiligheidsmaatregelen gebruik zullen maken van de verwerking van persoonsgegevens. Door de toenemende digitalisering van onze samenleving worden op steeds meer plaatsen gegevens vastgelegd. Deze gegevens kunnen ook gebruikt worden voor controledoeleinden. Denk hierbij aan

⁷ Een goed voorbeeld hiervan is het gebruik van het recht op privacy om de vrijheid van meningsuiting te waarborgen. Een wat meer basaal voorbeeld is het gebruik van het recht op privacy om hinder door ongewenste elektronische communicatie (spam) te voorkomen.

geautomatiseerde toegangscontrole met behulp van biometrische gegevens, (intelligent) cameratoezicht en datamining.

6.2.1 *De zorgvuldige verwerking van persoonsgegevens*

Willen veiligheidsmaatregelen waarbij persoonsgegevens worden verwerkt in overeenstemming zijn met het recht op privacy, dan zal de verwerking van deze gegevens op een zorgvuldige wijze plaats dienen te vinden. Hieronder zal daarom kort worden ingegaan op de uitgangspunten van de informationele privacy. Deze vloeien voort primair voort uit de OESO-richtlijn voor de bescherming van persoonsgegevens.⁸ De OESO-richtlijn vormde de basis voor de Europese richtlijn voor de bescherming van persoonsgegevens (95/46/EG). In Nederland heeft deze richtlijn zijn beslag gekregen in de Wet bescherming persoonsgegevens. De uitgangspunten van de OESO richtlijn, de EU richtlijn en de Wet bescherming persoonsgegevens zijn:

- *Limitering van het verzamelen van gegevens (collection limitation principle)*

Deze bepaling stelt dat er een limiet is aan de hoeveelheid gegevens die over een persoon verzameld mogen worden, en dat deze gegevens op rechtmatige en eerlijke wijze verkregen moet worden, waar noodzakelijk met de wetenschap of toestemming van de betrokkene.

- *Kwaliteit van de gegevensverwerking (data quality principle)*

Deze bepaling stelt dat persoonsgegevens noodzakelijk moeten zijn voor het doel waartoe ze verwerkt worden en voor dit doel compleet, nauwkeurig en up-to-date moeten zijn.

- *Doelbindingscriterium (purpose specification principle)*

Deze bepaling stelt dat het doel waarvoor persoonsgegevens verzameld worden niet later vermeld dient te worden dan het moment van verkrijging, en dat de persoonsgegevens enkel en alleen mogen worden verwerkt ten behoeve van dit doel, of doelen die met het oorspronkelijke doel verenigbaar zijn.

- *Beperking gebruik gegevens (use limitation principle)*

Deze bepaling stelt dat persoonsgegevens niet openbaar mogen worden gemaakt, verstrekt of anderszins gebruikt anders dan in overeenstemming met het doelbindingscriterium. Een uitzondering op deze regel is alleen mogelijk met de toestemming van de betrokkene of in de gevallen die bij de wet zijn voorzien.

- *Veiligheid en vertrouwelijkheid gegevens (security safeguards principle)*

Deze bepaling stelt dat er adequate veiligheidsmaatregelen genomen dienen te worden om persoonsgegevens te beschermen tegen ongeoorloofde toegang, vernietiging, gebruik, aanpassing of openbaring.

- *Openheid en transparantie (openness principle)*

Deze bepaling stelt dat er een algemeen beleid van openheid dient te zijn met betrekking tot ontwikkelingen, toepassingen en beleidsvorming op het gebied van de verwerking van persoonsgegevens. Het moet in afdoende mate mogelijk zijn om het bestaan en de aard van persoonsgegevens vast te stellen, alsmede de doelen voor het gebruik van persoonsgegevens. Verder moet het mogelijk zijn om de vestigingsplaats en de identiteit van de verantwoordelijke voor de verwerking vast te stellen.

- *Verantwoordelijkheid (accountability principle)*

Deze bepaling stelt dat de verantwoordelijkheid voor de verwerking van gegevens ligt bij de persoon of organisatie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze zogenoemde 'verantwoordelijke' moet er zorg voor dragen dat de verwerking in overeenstemming is met de wet.

6.3 **Privacy en publieke ruimte**

Van oudsher beperkt het recht op privacy zich tot de 'persoonlijke levenssfeer'. Net als het begrip 'privacy' valt ook van het begrip 'persoonlijke levenssfeer' moeilijk te duiden. Uit de Grondwet komt wel naar voren dat het begrip persoonlijke levenssfeer in ieder geval het lichaam, de woning en de correspondentie omvat.

Naast de persoonlijke levenssfeer onderscheidt de wet de openbare, publieke ruimte waar de burger over het algemeen geen beroep kan doen op het recht op privacy. Dit onderscheid is voor het Secure Haven pro-

⁸ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

gramma relevant omdat veel van de veiligheidsmaatregelen binnen Secure Haven betrekking zullen hebben op de publieke ruimte.

Het onderscheid tussen de publieke ruimte en de persoonlijke levenssfeer is echter niet zwart wit. Zo zijn er tal van situaties denkbaar waar de burger wel een beroep kan doen op (een conceptie van) het recht op privacy, ook al bevindt deze burger zich in een publieke ruimte. Omgekeerd is ook mogelijk: wanneer een burger zich in zijn woning bevindt kunnen er toch redenen zijn waardoor hij geen beroep kan doen op het recht op privacy.

In deze discussie speelt de doctrine van een ‘reasonable expectation of privacy’ een belangrijke rol, alsmede het concept informatiele privacy.

6.3.1 *De ‘reasonable expectation of privacy’*

De doctrine van de ‘reasonable expectation of privacy’ stamt uit het Amerikaanse recht. Het idee achter de reasonable expectation of privacy is dat door het feit dat er geen duidelijke scheiding is tussen publiek en privaat, bij twijfelgevallen aangesloten moet worden bij de subjectieve privacybeleving van de burger. Wanneer een burger zich door de gezagsdragers in zijn privacy voelt aangetast, dan kan hij een beroep doen op de bescherming die hem toekomt op grond van artikel 10 Grondwet. Wanneer een dergelijke subjectieve beleving vanuit een objectief perspectief als redelijk wordt beoordeeld, dan is er sprake van een privacyschending. Het reasonable expectation of privacy criterium kent dus twee elementen: 1) een subjectief element (de burger moet het idee hebben dat hij in zijn persoonlijke levenssfeer is aangetast, en 2) een objectief element (de aanspraak op de persoonlijke levenssfeer moet als redelijk worden beschouwd).

Een klassiek voorbeeld betreft een verdachte die in een publieke telefooncel wordt afgeluisterd. Ondanks dat de telefooncel een voor het publiek toegankelijke plaats is, mag de verdachte een bepaalde verwachting koesteren omtrent de privacy van het telefoongesprek. Het afluisteren van een dergelijk gesprek is daarmee in strijd met het recht op privacy.⁹

De verwerking van gegevens heeft een belangrijke invloed op de interpretatie van de reasonable expectation of privacy. In het klassieke denken over privacy vormen fysieke barrières tussen publiek en privaat (zoals de muren van een woning, of de kleding van een persoon) een belangrijke factor bij het bepalen of er sprake is van een inbreuk op de privacy. Wij zien dit ook duidelijk terug in de definities binnen het Wetboek van Strafvordering (Sv) waar bijvoorbeeld specifiek wordt gesproken over bevoegdheden in een besloten plaats (onder andere artikel 126k Sv) het onderzoek aan kleding (onder andere artikel 55a, artikel 56 en artikel 61c Sv). Echter, door de toenemende gegevensverwerkingen (zowel de verwerkingen die plaatsvinden in het ‘dagelijks leven’ als die specifiek ter uitvoering van de politietaak en het opsporen van strafbare feiten) die het gevolg zijn van het digitaliseren van onze (fysieke) leefruimte veranderen opvattingen over de reasonable expectation of privacy. Omdat mensen zich in toenemende mate bewust zijn van het feit dat hun persoonsgegevens in de publieke ruimte verwerkt kunnen worden, kalft de notie van de reasonable expectation of privacy steeds verder af. Dit wil echter niet zeggen dat het privacy begrip in de fysieke ruimte aan belang inboet. Via de bescherming van persoonsgegevens krijgt de bescherming van privacy in de fysieke ruimte alsnog gestalte.

6.3.2 *Informatiele privacy en de publieke ruimte*

Tegenstanders van het volgen en identificeren van personen in de publieke ruimte (bijvoorbeeld met behulp van beveiligingscamera’s) beroepen zich vrijwel altijd op het recht op privacy. Er is dus duidelijk een subjectieve ervaring van privacy in de publieke ruimte.¹⁰ Het is echter de vraag of deze privacywens gericht is op de bescherming van de persoonlijke levenssfeer zelf, of dat deze gericht is op het beschermen van achterliggende doelen zoals de persoonlijke autonomie. De idee om het recht op privacy in te roepen is in deze context dat de persoonlijke autonomie gewaarborgd blijft als gezagsdragers de mogelijkheid tot identificatie en volgen wordt ontzegd.¹¹

⁹ Katz v. The United States, 389 US 347, 351 (1967), zie ook: Lüdi v. Switzerland, EHRM, Judgment of 15 June 1992, Series A no 238

¹⁰ Voor een overzicht van de verhouding tussen privacy en het gebruik van beveiligingscamera’s zie: Dubbeld, 2004

¹¹ Zie voor een uitgebreide bespreking van dit concept hoofdstuk 10

Daar waar tot voor kort de anonimiteit van de massa en het feit dat het handelen van personen in de publieke ruimte niet werd gevolgd en vastgelegd, afdoende waarborgen vormden voor de handhaving van de persoonlijke autonomie, lijkt inmiddels de informationele privacy een effectiever en meer gebruikt mechanisme. De toepassing van veiligheidsmaatregelen moet in overeenstemming met de Wet bescherming persoonsgegevens geschieden. De in dit hoofdstuk genoemde uitgangspunten van het gegevensbeschermingsrecht zijn dus ook van toepassing op veiligheidsmaatregelen.¹²

¹² Het valt buiten de scope van deze rapportage om de werking van de Wet bescherming persoonsgegevens in zijn geheel uit te leggen. Hiervoor wordt verwezen naar de *Handleiding voor Verwerkers van Persoonsgegevens 2002* (zie www.cbpreweb.nl)

7 Veiligheid en opsporing binnen Secure Haven

In juridische zin kunnen veiligheidsmaatregelen op verschillende manieren gekwalificeerd en geassocieerd worden. Zo zijn er veiligheidsmaatregelen die voortvloeien uit privaatrechtelijke verhoudingen (de verplichte personeelspas vloeit bijvoorbeeld voort uit de arbeidsrelatie) en maatregelen die voortvloeien uit publiekrechtelijke verhoudingen (bijvoorbeeld het preventief fouilleren in risicogebieden).

Met het oog op het Secure Haven programma zal met name gekeken worden naar veiligheidsmaatregelen en daarmee geassocieerde bevoegdheden die vanuit de publiekrechtelijke taak worden geïnitieerd.¹³ Met het oog op het te bewerkstelligen doel kunnen we (in juridische zin) grofweg het volgende onderscheid maken in de bevoegdheden waarop (te nemen) veiligheidsmaatregelen zijn gebaseerd: 1) preventie en 2) opsporing. Het is hierbij nog van belang te melden dat veel veiligheidsmaatregelen verschillende doelen kunnen nastreven.

7.1 Preventie

Vanuit een economisch perspectief is de mate van veiligheid een rationele keuze waarbij verschillende belangen moeten worden afgewogen zoals kosten, gemak en toegankelijkheid.

Veel van de veiligheidsmaatregelen binnen Secure Haven zullen primair gericht zijn op de preventie van risico's. Als we de veiligheidsmaatregelen in ogenschouw nemen die gericht zijn op het voorkomen van risico's die voortvloeien uit bewust menselijk handelen, dan zien we dat deze hoofdzakelijk gericht zijn op het ontmoedigen van personen/organisaties die de veiligheid willen aantasten.

Wanneer we een potentiële crimineel of terrorist als een rationele actor beschouwen, dan zal deze een aantal elementen mee laten wegen in zijn beslissing om al dan niet een misdaad te plegen. Het gaat hierbij om vragen als:

- 1) wat levert het op (geldelijk gewin, status, politiek statement)?
- 2) welke investeringen moeten hiervoor gedaan worden?
- 3) hoe groot is de kans op succes?
- 4) wat is de pakkans?
- 5) wat is de straf?

Met andere woorden, de beslissing om een misdaad te plegen is veelal een kosten-batenanalyse. Veiligheidsmaatregelen zijn er op gericht om deze kosten-batenanalyse negatief uit te laten vallen voor de potentiële crimineel. Wanneer bijvoorbeeld het plegen van een inbraak in een woning grote investeringen aan tijd, apparatuur en organisatie vergt omdat er een effectief beveiligingssysteem aanwezig is, is het niet interessant om de inbraak te plegen als er slechts 100 euro in het nachtkastje van de bewoner ligt. De kosten-batenanalyse voor dezelfde inbraak kan echter heel anders uitvallen als de inbreker weet dat er zeer kostbare kunstschatten in het huis aanwezig zijn. Ditzelfde geldt voor de tasjesdief die weet dat hij door de slimme bewakingscamera's in een winkelstraat makkelijk te identificeren en te traceren is. In dit geval is de pakkans te hoog om de diefstal van een kleine buit te rechtvaardigen. Wanneer deze camera's niet aanwezig zijn dan kan de tasjesdief besluiten dat zelfs een kleine buit de moeite waard is omdat de pakkans toch gering is.

Voor terroristische misdrijven gelden andere drijfveren dan voor 'normale' misdrijven. Dit betekent ook dat terroristen op een andere wijze tegen de hierboven geschetste kosten-baten analyse aan zullen kijken. Met name de rationele economische argumenten (de verhouding investering-opbrengst) zullen van minder groot belang zijn. Een terrorist zal wellicht ook minder geven om de straf of de pakkans en het doel van zijn terroristische actie boven alles stellen (Mohammed B. en Volkert van der G. zijn hier goede voorbeelden van). De hierboven genoemde preventieve werking die van camera's uitgaat is bij terroristische misdrijven dan bij

¹³ Hoewel de handhaving van de openbare orde en veiligheid een publiekrechtelijke taak is (uitgevoerd op initiatief van het College van B&W), kan voor de uitvoering van deze taak ook worden aangesloten bij de private sector. Hierbij kan gedacht worden aan co-regulering en de inzet van private middelen voor publieke doeleinden (via bijvoorbeeld particuliere beveiligingsdiensten). Uiteraard speelt de private sector zelf ook een rol bij het zorg dragen voor veiligheid.

voorbeeld ook irrelevant.¹⁴ Een terrorist zou echter misschien wel afgeschrikt kunnen worden door een strenge toegangscontrole omdat deze zijn kansen op succes verlagen.

Veiligheidsmaatregelen zijn als zodanig veelal gericht op de preventie van deviant gedrag en het voorkomen van strafbare gedragingen. Vanuit de gedachte dat gelegenheid de dader maakt, wordt door middel van (zichtbare) veiligheidsmaatregelen het signaal gegeven aan potentiële daders dat zij in de gaten worden gehouden en dat de aanwezige veiligheidsmaatregelen bijzonder krachtig zijn. Bij preventieve veiligheidsmaatregelen kan onder andere gedacht worden aan patrouillerende agenten (blauw op straat), preventief fouilleren en cameratoezicht. Al deze maatregelen zijn gericht op het handhaven van de openbare orde en veiligheid.

De bevoegdheid tot het nemen van preventieve veiligheidsmaatregelen is (onder andere) vastgelegd in een aantal wetten waaronder het Wetboek van Strafvordering, de Politiewet, de Gemeentewet, de Wet Wapens en Munitie, de Wet op het Cameratoezicht en de Wet op de Identificatieplicht.

Het betreft hier veelal algemene uitgangspunten en bevoegdheden (wat mag een opsporingsambtenaar bijvoorbeeld wel of niet) die niet specifiek aan de gemeente Den Haag zijn gebonden. Wel heeft de gemeente een sterke zelfstandige rol bij het stellen van regels en het nemen van beslissingen met het oog op het bewaken van de openbare orde in Den Haag. Deze regels en besluiten zijn vastgelegd in de Algemene Politieverordening (APV) van 's Gravenhage. Het gaat dan onder meer om:

- 1) cameratoezicht (hfdst 2, afdeling V, APV 's Gravenhage),
- 2) regels omtrent samenscholingen (hfdst 2, afdeling I, § 4, APV 's Gravenhage)
- 3) regels omtrent openbare manifestaties (hfdst 2, afdeling I, § 5, APV 's Gravenhage)
- 4) het aanwijzen van 'veiligheidsrisicogebieden' waarbinnen preventief fouilleren mogelijk is (hfdst 2, afdeling IV, artikel 76c, APV 's Gravenhage)

7.1.1 De zelfstandigheid van de Internationale Zone

De aparte status van de Internationale Zone binnen de gemeente Den Haag brengt met zich mee dat er ook andere veiligheidsprioriteiten aan toegekend kunnen worden. Zo bestaat de mogelijkheid om de Internationale Zone door het Kabinet aan te laten wijzen als 'permanent veiligheidsgebied'. Preventieve veiligheidsmaatregelen zoals de bevoegdheid tot het preventief fouilleren kunnen aldus permanent gelden binnen de Internationale Zone.

Voor de veiligheidsbeleving van de bezoekers en inwoners van de Internationale Zone kan een dergelijke beslissing relevant zijn. Zowel in positief als in negatief opzicht. Zo kan de veiligheidsperceptie van de bezoekers en inwoners stijgen (hun leef- en werkomgeving wordt beter bewaakt dan andere gebieden in Nederland). De veiligheidsbeleving kan ook dalen (burgers hebben het gevoel dat zij binnen de internationale zone constant in de gaten gehouden worden).¹⁵

7.1.2 Relevantie voor Secure Haven

Veiligheidsmaatregelen die gericht zijn op de handhaving van de veiligheid en de openbare orde binnen de gemeente Den Haag vanuit een preventief opzicht zijn voor het Secure Haven programma het meest interessant. De reden hiervoor is dat de bevoegdheid tot het nemen van dergelijke maatregelen grotendeels bij de gemeente zelf ligt. De gemeente heeft dus (binnen de grenzen van de wet) relatieve autonomie bij het invoeren van preventieve veiligheidsmaatregelen.

7.2 Opsporing

Uiteraard zijn veiligheidsmaatregelen nooit honderd procent effectief en kan het dus voorkomen dat een misdaad alsnog plaatsvindt. Het is dan zaak om de misdaad op te lossen. Puur vanuit het idee van veiligheid

¹⁴ Het feit dat één van de twee grootste terroristische aanslagen op Europa uit de recente geschiedenis (7 juli 2005) in London plaatsvond, de stad met het meeste cameratoezicht ter wereld, is hier een schrijnend voorbeeld van.

¹⁵ Zoals eerder aangegeven is het binnen dit werpakket niet goed mogelijk om relevante uitspraken te doen over de veiligheidsbeleving van de bezoekers en inwoners van de Internationale Zone.

en openbare orde is dit van belang, omdat hiermee invulling wordt gegeven aan de generaal preventieve werking die uit moet gaan van het strafrecht.

De opsporingstaak wordt ingevuld door opsporingsambtenaren. Om hun taak goed te kunnen uitvoeren hebben opsporingsambtenaren meer bevoegdheden dan de gemiddelde burger. Het gaat dan specifiek om opsporingsbevoegdheden en dwangmiddelen. Deze zijn vastgelegd in onder andere de Politiewet en het Wetboek van Strafvordering.¹⁶

In de opsporing kan een onderscheid worden gemaakt tussen opsporing nadat een misdaad is gepleegd (reactieve opsporing) en opsporing die plaatsvindt ter voorkoming van misdrijven (pro-actieve opsporing).

7.2.1 *Reactieve opsporing*

Reactieve opsporing (ook wel opsporing in klassieke zin) is waarheidsvinding die gericht is op het oplossen van strafbare feiten.

Door de komst van ICT is het aantal beschikbare sporen sterk toegenomen. Hierbij kan onder gedacht worden aan gegevens van de mobiele telefoon, internetgegevens, gegevens uit PDA's, camerabeelden en informatie in databases van derden. Al deze gegevens kunnen gebruikt worden om het proces van waarheidsvinding te ondersteunen. Daarnaast is de toegankelijkheid van *bestaande* sporen verbeterd door de inzet van zoekmachines gecombineerd met databanken. Wanneer we kijken naar veiligheid binnen Secure Haven mogen dus we constateren dat het gebruik van ICT-middelen in de publieke ruimte het ophelderingspercentage kan verhogen.

De bevoegdheden die geassocieerd kunnen worden met de reactieve opsporing liggen besloten in de Politiewet en het Wetboek van Strafvordering. Met het oog op toekomstige veiligheidsmaatregelen zoals intelligente camera's en automatische identificatietoepassingen zijn met name de bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering (eerste boek, titel IVa Sv) interessant. Het gaat dan met name om het onderzoeken van telecommunicatie (eerste boek, titel IVa, zevende afdeling Sv) en het vorderen van gegevens (eerste boek, titel IVa, achtste afdeling Sv).

7.2.2 *Pro-actieve opsporing*

Pro-actieve opsporing behelst het inzetten van opsporingsbevoegdheden met het oog op de voorkoming van ernstige strafbare feiten, waaronder terrorisme. Het idee bij deze vorm van opsporen is dat gezien het ernst van de (te plegen) strafbare feiten waarnaar onderzoek wordt gedaan voorkomen beter dan genezen is. Het gaat hierbij veelal om vergaande opsporingsbevoegdheden zoals datamining en infiltratie die potentieel een grote invloed kunnen hebben op de grondrechten van de burger.

De bevoegdheden tot pro-actief opsporen zijn in het wetboek van Strafvordering geregeld in het eerste boek, titel V en Vb.

7.2.3 *Relevantie voor Secure Haven*

Hoewel opsporing van groot belang is voor de handhaving van de veiligheid en de openbare orde is de zelfstandige relevantie van dit onderwerp minder groot voor het Secure Haven programma. De reden hiervoor ligt in het feit dat de bevoegdheden die met de opsporing geassocieerd zijn niet op gemeentelijk niveau vastgesteld kunnen worden. Uiteraard zijn beide onderwerpen wel relevant wanneer het gaat om de concrete invulling binnen de gemeente en de prioriteiten die binnen de gemeente aan bepaalde politietaken worden gegeven.

7.3 **Gegevensverwerkingen binnen Secure Haven**

Zoals reeds eerder in deze rapportage aan de orde is gekomen, zal voor de effectiviteit van veel veiligheidsmaatregelen het verwerken van (persoons)gegevens onontbeerlijk zijn. Dit geldt zowel voor veiligheidsmaatregelen die vanuit de publieke taak geïnitieerd zijn, als die vanuit private ondernemingen zijn gestart. Met het oog op zowel reactieve en pro-actieve opsporing is het van belang te vermelden dat deze gegevens onder

¹⁶ Opsporingsbevoegdheden kunnen bijvoorbeeld ook voortvloeien uit een bestuursrechtelijke taak en/of het financieel economisch strafrecht. Met het oog op het doel en de omvang van deze rapportage zullen deze bevoegdheden buiten beschouwing worden gelaten.

omstandigheden ook ingezet kunnen worden voor de opsporingstaak. Zo kunnen op grond van de Wet vorderen gegevens in het kader van onderzoek naar georganiseerde criminaliteit en terroristische misdrijven, persoonsgegevens worden gevorderd.¹⁷ Deze mogelijkheid kan enerzijds bijdragen aan de veiligheid, maar anderzijds additionele druk leggen op de bescherming van grondrechten binnen Secure Haven. Bij de beoordeling hoe een veiligheidsmaatregel zich verhoudt tot de grondrechten van de burger, dient deze bredere context ook meegewogen te worden.

¹⁷ Wet bevoegdheden vorderden gegevens, *Staatsblad* 2005, 390

8 Technologische ontwikkelingen

Zoals uit de voorgaande hoofdstukken reeds naar voren is gekomen, speelt de verwerking van (persoons)gegevens een belangrijke rol bij de toepassing van veiligheidsmaatregelen. Met het oog op deze constatering is het van belang te kijken hoe de technologische vooruitgang op het gebied van informatie- en communicatietechnologie (ICT) gestalte krijgt en welke invloed dit heeft op de ontwikkeling van Secure Haven. Het is moeilijk om erg ver in de toekomst te kijken wanneer het gaat om het maken van beleid. Zeker bij het onderwerp van deze rapportage bestaat al snel de neiging om te vervallen in utopische dan wel dystopische scenario's. Toch zijn er wel een aantal trends waarneembaar die voor de ontwikkeling van Secure Haven richting 2017 relevant zijn.¹⁸

Twee trends zijn voor het onderwerp van deze rapportage met name van belang: 1) de alomtegenwoordigheid van ICT, en 2) een betere informatiehuishouding. De eerste trend is van belang omdat de hoeveelheid verwerkte gegevens hierdoor sterk toe zal nemen, de tweede trend is van belang omdat een goede informatiehuishouding noodzakelijk is om ook daadwerkelijk informatie en kennis aan deze gegevens te ontfemen. Dit betekent waarschijnlijk een vergroting van de veiligheid (risico's zijn immers beter in te schatten en te controleren), maar zal mogelijk ook de bescherming van grondrechten onder druk zetten.

8.1 Alomtegenwoordigheid ICT

Door de ontwikkeling van kleinere en krachtigere microprocessoren kunnen steeds meer objecten worden uitgerust met computerkracht. Hierdoor wordt computerkracht steeds meer een alomtegenwoordig fenomeen. Dit wordt ook wel *ubiquitous of pervasive computing* genoemd (Schermer 2008, p. 13). De aanwezige computerkracht wordt ontsloten en verbonden met behulp van netwerktechnologie. Door een combinatie van technologieën (waaronder (mobiel) internet, RFID, NFC en sensoren) en inzichten uit de psychologie en de cognitieve wetenschappen wordt het zelfs mogelijk om de fysieke wereld 'bewust' te maken van de aanwezigheid van gebruikers. De alomtegenwoordige, intelligente en onzichtbare ICT-infrastructuur kan anticiperen en reageren al naar gelang de wensen en de behoeften van personen. We spreken dan van *ambient intelligence* (Aarts *et al.* 2002).

Door de alomtegenwoordigheid van ICT en onze afhankelijkheid als maatschappij ervan, neemt het aantal plaatsen waar wij in contact komen met ICT toe. Over het algemeen worden deze contactmomenten vastgelegd. Hierbij kan onder andere worden gedacht aan een elektronische betaling, reizen met de OV-chipkaart, langs een bewakingscamera lopen en het surfen op internet. Tijdens deze vele interacties met ICT laten we bewust en onbewust (persoons)gegevens achter. Deze 'informatievoetstappen' zijn noodzakelijk om het dagelijks leven in de informatiemaatschappij mogelijk te maken, maar zij kunnen ook gebruikt worden voor opsporingsdoeleinden.

Het valt te verwachten dat ook binnen Secure Haven processen sneller, veiliger en eenvoudiger voor bewoners en bezoekers worden gemaakt met behulp van ICT. Als zodanig zullen vele informatievoetstappen van personen worden vastgelegd en opgeslagen binnen Secure Haven. Het gaat hierbij zowel om ICT-infrastructuren die voor private doeleinden worden aangewend (bijvoorbeeld kassa's en klantenkaarten) als die voor publieke doeleinden worden aangewend (variërend van de gemeentelijke basisadministratie tot bewakingscamera's).

8.2 Verbeterde informatiehuishouding

Grote hoeveelheden data dragen op zichzelf niet bij aan een betere informatiepositie voor de politie en/of de gemeente. Uit de grote hoeveelheden ruwe data die binnen Secure Haven beschikbaar komen, dient namelijk eerst nog informatie afgeleid te worden. Deze informatie moet vervolgens in een bepaalde context geplaatst worden voordat er sprake is van kennis: informatie waar ook daadwerkelijk wat mee gedaan kan worden. Met name deze laatste stap is lastig. De enorme berg data die is ontstaan binnen de informatiemaatschappij

¹⁸ Voor een indruk hoe veiligheidsmaatregelen in 2017 gestalte kunnen krijgen, wordt verwezen naar de scenario's in de appendix bij dit rapport.

heeft geleid tot het probleem van *information overload*, ofte wel, te veel informatie om nog wijs uit te kunnen worden.

Voorts speelt het probleem dat verschillende organisaties informatie veelal niet of niet effectief met elkaar delen. Hierdoor kan het voorkomen dat hoewel alle benodigde informatie beschikbaar is, er toch niet effectief gehandeld wordt, omdat men 'de puntjes niet met elkaar kan verbinden'. Nergens werd dit probleem duidelijker zichtbaar dan bij de aanslagen van 11 september 2001. Uit het onderzoek naar de aanslagen van 11 september kwam naar voren dat reeds voordat de aanslagen plaatsvonden bij de diverse opsporings- en inlichtingendiensten (FBI, CIA en NSA) in principe genoeg informatie aanwezig was om een duidelijk beeld te krijgen van de plannen van de terroristen. Door een onfortuinlijke combinatie van onkunde, inefficiëntie en onwelwillendheid om informatie te delen werden de cruciale waarschuwingssignalen niet in hun onderlinge samenhang gezien en niet in de juiste context geplaatst (Kean 2004).

Diverse organisatorische en technologische ontwikkelingen moeten de informatiehuishouding van inlichtingen- en opsporingsinstanties verbeteren. Onder andere in het onderzoeksveld van de kunstmatige intelligentie (AI) worden stappen gezet om beter om te kunnen gaan met grote hoeveelheden informatie. Naast technologische vooruitgangen, groeit ook het organisatorisch en institutioneel besef dat informatie beter verwerkt en gedeeld moeten worden. De verwachting is dan ook dat richting 2017 niet alleen meer data beschikbaar zal zijn, maar dat deze ook beter verwerkt en in perspectief geplaatst kan worden.

8.3 Veiligheidsmaatregelen richting 2017

Op basis van de hierboven beschreven trends (meer data en betere verwerkingscapaciteit) zullen hieronder enkele veiligheidsmaatregelen worden besproken die voor de context van Secure Haven relevant zijn. Deze maatregelen zullen in de toekomst sterk beïnvloed worden door de technologische en organisatorische ontwikkelingen. Het verdient de nadruk om te zeggen dat het hier alleen gaat om informatiegebaseerde veiligheidsmaatregelen die de capaciteit tot toezicht (surveillance en inzicht van de politie/gemeente) moeten helpen verstevigen.

8.3.1 Monitoring

Een belangrijk element binnen het Secure Haven concept is het verkleinen en beheersen van risico's. Preventie door toezicht op de publieke ruimte (monitoring) is één van de maatregelen om de veiligheid te vergroten. Cameratoezicht is het bekendste voorbeeld van monitoring.

Wil monitoring effectief zijn, dan dienen de beelden in real-time geïnterpreteerd moeten worden door menselijke operators. Deze operators beoordelen wat afwijkend gedrag is, wie verdacht is *et cetera*. Menselijke operators hebben echter twee nadelen: 1) ze zijn niet goed in het verwerken van grote informatiestromen en 2) ze hebben een beperkte aandachtsspanne.¹⁹

Hoe groter de toestroom van informatie, hoe moeilijker het wordt voor de operator om al deze informatie te verwerken. Het gevolg is *information overload*: de operator verdrinkt in de beschikbare informatie en kan niet langer zijn taak goed uitoefenen. Het tweede probleem betreft de aandachtsspanne van mensen. Mensen kunnen slechts voor een beperkte tijd goed informatie verwerken, na verloop van tijd verslapt de aandacht.

Tot op heden was de oplossing voor deze twee problemen de inzet van extra mankracht. Vanzelfsprekend brengt dit hoge kosten met zich mee. Vanuit het oogpunt van effectiviteit en efficiency is het dus zinvol om te kijken naar technologische oplossingen en alternatieven. Deze alternatieven zijn er in toenemende mate door ontwikkelingen op het gebied van kunstmatige intelligentie. 'Slimme camera's' bijvoorbeeld, die verdachte personen, gedragingen of situaties kunnen herkennen, zullen richting 2017 steeds vaker worden ingezet. Voordeel van deze slimme camera's is dat zij beter om kunnen gaan met *information overload* en 24 uur per dag actief zijn.

Richting 2017 zullen ook verschillende typen sensoren (naast beeld bijvoorbeeld geluidssensoren en warmtesensoren) worden geïntegreerd. Zo wordt het mogelijk om bijvoorbeeld een camera alleen te activeren wanneer deze tekenen van geweld waarneemt (schreeuwende mensen, pistoolschoten).

¹⁹ Een derde probleem dat hier verder niet besproken zal worden is het feit dat de interpretatie van de beelden door menselijke operators altijd een subjectief element bevat.

8.3.2 *Intelligence led policing*

De politie heeft beperkte middelen. Het is daarom zaak deze middelen zo effectief mogelijk in te zetten. Naar mate de politie meer weet over wat er binnen Secure Haven allemaal gebeurt (hoeveel personen bezoeken het Vredespaleis, waar en wanneer vinden de meeste geweldsmisdrijven plaats, hoe lopen de mensenstromen tijdens Koniginnenach), is zij beter haar middelen alloceren. Informatie die gebruikt kan worden om de beslissingen van de politie te sturen is cruciaal voor dit proces, vandaar dat deze benadering wordt aangeduid met de term intelligence led policing. Naarmate er meer ICT wordt toegepast zal meer data beschikbaar komen. Met behulp van data-mining en andere analyse methoden kunnen deze data informatie opleveren over wat er allemaal in Secure Haven plaatsvindt. Het is dus de verwachting dat richting 2017 de politie haar middelen dankzij intelligence led policing effectiever zal kunnen inzetten.

8.3.3 *Datamining en profiling*

Om ernstige misdaden en terroristische aanslagen te voorkomen moeten de voorbereidingshandelingen voor dergelijke misdaden en aanslagen in een vroeg stadium herkend worden. Met behulp van allerlei technieken zoals data-mining, opponent modelling en netwerk-analyse, proberen inlichtingen- en opsporingsdiensten pro-actief op te sporen. Door bijvoorbeeld uit de *modus operandi* van drugsmokkelaars bepaalde terugkerende handelingen te destilleren, kan een patroon worden opgesteld van een typische drugsdeal. Vervolgens kan met behulp van data-mining gezocht worden naar dit patroon in beschikbare data. Wanneer een gelijkend profiel (een match) is gevonden, is dit een eerste indicatie dat er mogelijk drugs worden gesmokkeld. Een ander voorbeeld is het in kaart brengen van criminele netwerken en terroristische cellen aan de hand van de relaties en communicatiepatronen tussen verschillende personen.

8.3.4 *Real time monitoring en data-sharing*

Data-mining en profiling kunnen waardevolle aanknopingspunten bieden voor de opsporing, maar hebben als nadeel dat zij niet in real-time plaatsvinden. Dit betekent dat de analyse niet kan plaatsvinden met de meest actuele informatie. Een ander probleem betreft de uitwisseling van gegevens. Voor een effectieve uitvoering van de politietaak is het van belang om accurate en actuele informatie te hebben. Het is daarom van belang dat data die op verschillende plekken door verschillende organisaties/entiteiten ingewonnen wordt effectief te delen (wederom in realtime). Om deze twee problemen te adresseren wordt hard gewerkt aan technieken die het mogelijk maken om in realtime grote hoeveelheden gegevens te verwerken en te delen. Hoewel deze vormen van realtime informatieverwerking nog in de kinderschoenen staan, zullen zij richting 2017 waarschijnlijk een belangrijke bijdrage leveren aan de veiligheid binnen Secure Haven.

8.4 **Tussenconclusie**

Hoewel de kracht en effectiviteit niet overschat moet worden, kan technologie wel degelijk een belangrijke bijdrage leveren aan de opsporing. Met name het effectief verwerken en delen van informatie binnen Secure Haven wordt richting 2017 van steeds groter belang.

Het slimme gebruik van ICT zal de capaciteit van de politie en gemeente om de veiligheid en openbare orde te handhaven binnen Secure Haven ongetwijfeld vergroten. Maar de toenemende 'informatiemacht' maakt de kans op schendingen van grondrechten groter en potentieel ernstiger. Wat de mogelijke risico's zijn van deze ontwikkeling wordt in het volgende hoofdstuk beschreven.

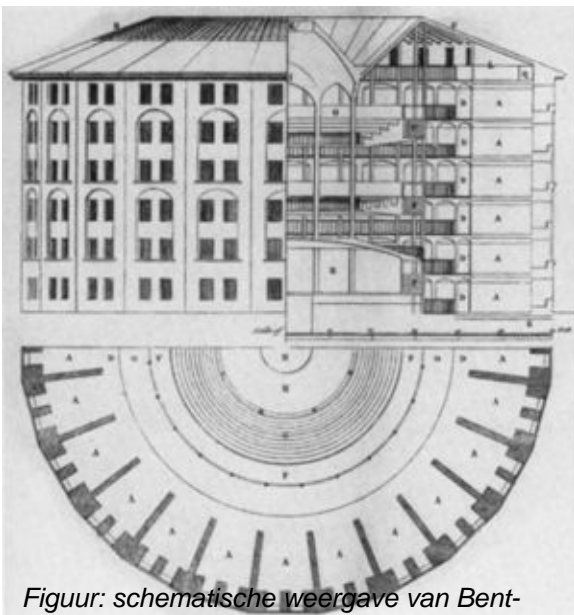
9 Risico's voortvloeiend uit veiligheidsmaatregelen

Met het oog op datgene wat in de afgelopen hoofdstukken de revue is gepasseerd, is het nu zaak om te kijken hoe het veiligheidsbelang en de grondrechten van de burger binnen de Secure Haven optimaal verenigd kunnen worden. Hiertoe zal in dit hoofdstuk een algemene analyse worden gemaakt van de mogelijke risico's die veiligheidsmaatregelen met zich mee kunnen brengen. De hier geconstateerde risico's gelden voor de introductie van veiligheidsmaatregelen in het algemeen.

Voor alle veiligheidsmaatregelen geldt dat het primaire risico dat zij in zich dragen een verschuiving in de machtsbalans tussen de overheid en haar burgers is. Door de introductie van veiligheidsmaatregelen worden de mogelijkheden van de overheid tot toezicht en controle vergroot, waardoor de burger effectiever kan ingrijpen in het leven van de burger. Deze verschuiving van macht vormt een rode draad door alle hieronder genoemde potentiële risico's.

9.1 Preventief: het Panopticon²⁰

Preventieve veiligheidsmaatregelen vormen de kern van de maatregelen die binnen Secure Haven genomen (kunnen) worden. Het gaat dan hoofdzakelijk om het toezicht houden op burgers en het uitstralen van dit toezicht. Het belangrijkste risico dat preventief toezicht in zich bergt is dat het zich steeds verder uitbreidt (creep) en meer 'alomtegenwoordig' wordt. In de surveillance theorie (een stroming binnen de sociologie) wordt dit aangeduid met de term 'super panoptisch' (Poster, 1990).



Figuur: schematische weergave van Bentham's Panopticon

Het Panopticon (Grieks voor alziend) was een gevangenismodel ontwikkeld door Jeremy Bentham (1843). Centraal in het ontwerp stond de totale zichtbaarheid en transparantie van de gevangene. De gevangenis bestond uit een ronde koepel met in het midden een centrale controletoeren. De cellen waren aan de voorzijde open zodat vanuit de centrale toren ten alle tijden gezien kon worden wat de gevangene aan het doen was. Dit maakte het uitvoeren van totale controle op de gevangene mogelijk.

Echter, naast de externe controle door de bewakers maakte het ontwerp van het Panopticon ook een meer subtiele vorm van controle mogelijk: die van controle door de gevangenen zelf. Omdat de gevangenen altijd zichtbaar waren, kwamen zij er al snel achter dat afwijkend of ongewenst gedrag niet verborgen kon worden en direct gesanctioneerd werd. Het feit dat letterlijk alles gezien en bestraft kon worden zorgde ervoor dat gevangenen op een gegeven moment zich niet meer afwijkend gingen gedragen, omdat zij de wetenschap hadden dat de pakkans 100% was. De gevangenen reguleerden als het ware zichzelf en internaliseerde het volledige normen- en waardenpakket van de toezichthouders (Foucault, 1995).

Deze laatste vorm is uiteraard een veel subtielere (en gevaarlijkere) vorm van controle. Hoewel het Panopticon als uitgangspunt voor veel gevangenisontwerpen is gebruikt (de meeste koepelgevangenisontwerpen zijn gebaseerd op het Panopticon) is het ontwerp van Bentham nooit in zijn totaliteit doorgevoerd, omdat dit te dehumaniserend voor de gevangenen bleek.

Het toenemende (elektronische) toezicht in de fysieke ruimte vertoont overeenkomsten met het idee van het Panopticon, maar dan op de schaal van de maatschappij als geheel. Vandaar dat surveillance en toezicht in

²⁰ De in deze paragraaf opgesomde risico's manifesteren zich ook bij de reactieve en pro-actieve opsporing, maar zullen aldaar niet nogmaals besproken worden.

de publieke ruimte ook wel wordt omschreven als ‘super panoptisch’. Hoewel het empirisch toetsen van deze theorie vooralsnog moeilijk is (er is immers nog geen super Panopticon) kan het ons wel richting geven bij het beschrijven van mogelijke risico’s en onwenselijke gevolgen voor Secure Haven.

9.1.1 *Verschuiving van de machtsbalans*

Het belangrijkste risico van het super Panopticon is de verschuiving van de machtsbalans. Omdat de norm wordt bepaald door de overheid en normconformisme binnen een Panopticon automatisch door de subjecten wordt geïnternaliseerd, is het een zeer krachtig middel om de burger te controleren.

Naast de macht die een super Panopticon verschaft aan het gezag heeft geïnternaliseerd normconformisme mogelijk ook tot gevolg dat het publieke leven verstart. Omdat burgers weten dat het afwijken van de norm vastgelegd wordt, zullen zij minder snel geneigd zijn om hun eigen gang te gaan uit angst voor veroordeling door de massa of mogelijk zelfs strafrechtelijke vervolging. Het resultaat is een conformistische samenleving met weinig plek voor diversiteit. Een dergelijk scenario tast de leefbaarheid en uiteindelijk zelfs de wenselijkheid van een Secure Haven aan.

9.1.2 *Sociale cohesie en discriminatie*

Een mogelijk risico dat de grootschalige invoering van veiligheidsmaatregelen met zich mee kan brengen is dat van een ongewenste scheiding tussen typen of groepen burgers. Een onderscheid dat voortvloeit uit de ‘veiligheidsstatus’ van burgers. Binnen Secure Haven bestaat aldus het risico op een ‘maatschappelijke schifting’ waarbij onderscheid wordt gemaakt tussen risicoburgers, gewone burgers en geprivilegieerden.²¹

Risicoburgers zijn die burgers die als een potentieel risico voor de veiligheid worden gezien omdat zij afwijken van de ‘norm’. Veiligheidsmaatregelen worden over het algemeen vaker ingezet tegen hen omdat zij bepaalde kenmerken hebben die indicatief zijn voor een verhoogd risico. Hierbij kan gedacht worden aan hangjongeren, linkse of rechtse activisten, maar bijvoorbeeld ook aan religieuze of etnische minderheden zoals moslims en Antillianen. Het bestempelen van burgers tot risicoburger op basis van uiterlijke of religieuze kenmerken is in strijd met het recht op gelijke behandeling.

Aan de andere kant van het spectrum staan de geprivilegeerde burgers. Deze burgers kunnen op grond van een bepaalde status (bijvoorbeeld inkomen of verbondenheid aan een internationale organisatie) meer voordelen genieten dan risicoburgers en gewone burgers (bijvoorbeeld omdat zij zich mogen onttrekken aan veiligheidsmaatregelen of voorrang krijgen).

Hoewel burgers qua rechten en verplichtingen binnen Secure Haven nooit helemaal gelijk zijn, moet onnodig kunstmatig onderscheid tussen burgers zoveel mogelijk voorkomen worden. Een dergelijk artificieel onderscheid tussen burgers is namelijk in strijd met het recht op gelijke behandeling en kan afbreuk doen aan de sociale cohesie binnen Secure Haven.

9.1.3 *Transparantie en democratische borging*

Een risico dat de vergaande invoering van (preventieve) veiligheidsmaatregelen verder met zich brengt is het verlies aan transparantie en democratische borging. Het is veelal voor de burger onduidelijk met welk doel preventieve veiligheidsmaatregelen worden ingevoerd, wie de regie over deze maatregelen en middelen voert en hoe de controle op deze maatregelen en middelen verloopt. Dit is niet enkel een bedreiging voor de legitimiteit van de veiligheidsmaatregelen, maar mogelijk ook voor de acceptatie ervan. Hoewel burgers een groot vertrouwen in de overheid hebben en over het algemeen de introductie van veiligheidsmaatregelen toejuichen (zie bijvoorbeeld *het Nationaal Vrijheidsonderzoek 2007*), kan deze houding veranderen door een onzorgvuldige of overmatige toepassing van veiligheidsmaatregelen.²²

9.2 **Opsporing: reactief**

Reactieve opsporing richt zich op waarheidsvinding en het opsporen van de daders van een strafbaar feit. Hoewel reactieve opsporing van groot belang is voor de veiligheid en leefbaarheid van Secure Haven zijn er weinig tot geen mogelijkheden voor de gemeente Den Haag om zelfstandig bevoegdheden te veranderen

²¹ De term geprivilegieerde wordt hier generiek gebruikt en doelt niet noodzakelijkerwijs op diplomatieke of consulaire medewerkers.

²² Stichting Nationaal Comité 4 en 5 mei (2007), *Nationaal Vrijheidsonderzoek 2007, Opiniedeel*.

en/of toe te voegen die de opsporing effectiever maken. Ruimte die de gemeente Den Haag wel heeft, heeft met name betrekking op het toekennen van prioriteit bij het oplossen van bepaalde typen misdrijven.

Waar wel mogelijkheden liggen (en daarmee risico's) is het vergemakkelijken van het verkrijgen van sporen. In de digitale wereld wordt het namelijk steeds beter mogelijk om digitale sporen van een misdrijf te vinden. Voorbeelden zijn camerabeelden, telefoongegevens en computerbestanden. Hoewel de vastlegging van dergelijke sporen voor de opsporing (en daarmee veiligheid) van wezenlijk belang zijn, bergt het vastleggen en gebruiken van deze sporen ook risico's in zich.

9.2.1 Inmenging in de persoonlijke levenssfeer

Een eerste risico is de toenemende inmenging in de persoonlijke levenssfeer van de burger. Naast de hinder die een burger hier mogelijk van kan ondervinden (bijvoorbeeld wanneer er vergissingen worden gemaakt bij de opsporing), kan ook de machtsbalans tussen burger en overheid langzaam verschuiven. Immers, kennis is macht en hoe meer gegevens worden vastgelegd, hoe meer mogelijkheden de overheid krijgt tot het omzetten van deze gegevens in kennis.

9.2.2 Function- en mission creep

Daarnaast bestaat er bij reactieve opsporing ook altijd het risico op function creep en mission creep. Dit houdt in dat een bevoegdheid en/of maatregel die voor het ene doel in het leven is geroepen in een later stadium alsnog voor een ander doel wordt gebruikt. De toepassing van een bestaande bevoegdheid of een bestaande maatregel gaat veelal niet gepaard met de democratische legitimatie die daarvoor noodzakelijk is.

9.3 Opsporing: pro-actief

Voor de pro-actieve opsporing geldt in wezen hetzelfde als voor de reactieve opsporing: met betrekking tot de bevoegdheden tot pro-actieve opsporing zijn er weinig tot geen mogelijkheden voor de gemeente Den Haag om zelfstandig de bevoegdheden op dit gebied te creëren. Wel is het mogelijk om de pro-actieve opsporing zo goed mogelijk te faciliteren met behulp van preventieve veiligheidsmaatregelen. Toch is het nuttig om in het bredere perspectief van veiligheid en grondrechten te kijken naar de risico's die pro-actieve opsporing met zich mee kan brengen.

Pro-actieve opsporing speelt met name een rol bij de opsporing van terroristische misdrijven. Technologische ontwikkelingen op het gebied van informatieverwerking zoals besproken in hoofdstuk 8 werken de toepassing van pro-actieve opsporing in de hand.

9.3.1 Risicojustitie

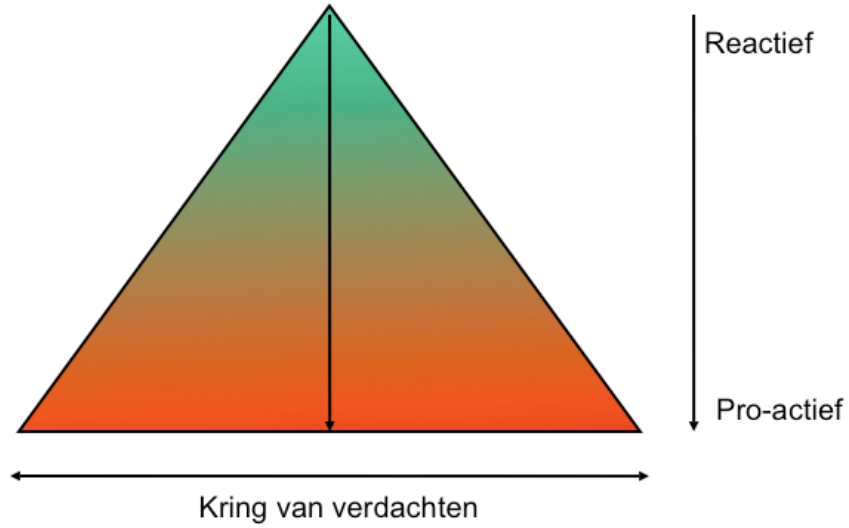
Het belangrijkste risico van pro-actieve opsporing is de verschuiving van schuld naar intentie. Omdat pro-actieve opsporing gericht is op het voorkomen van strafbare feiten in plaats van het reactief opsporen ervan, moeten reeds in een vroeger stadium opgespoord worden. Onder het mom van 'voorkomen is beter dan genezen' worden daarbij reeds in een vroeg stadium opsporingsmiddelen en bevoegdheden ingezet die een serieuze bedreiging kunnen vormen voor de grondrechten van de burger. Deze ontwikkeling wordt aangeduid met de term risicojustitie (Cleiren, 2006).

Gegeven het feit dat er dus nog geen sprake is van onomstotelijk bewijs dat een verdachte daadwerkelijk een strafbaar feit gaat plegen, bestaat het risico op vergissingen. Zo kan bijvoorbeeld iemand die niks kwaads in de zin heeft alsnog op basis van een aantal risicocriteria als verdacht worden beschouwd. Dit is de problematiek van de zogenaamde 'vals positieven'. Andersom is natuurlijk ook mogelijk: op basis van een aantal risicocriteria wordt iemand ten onrechte beschouwd als niet gevaarlijk. We hebben het dan over vals negatieven.

De mogelijkheid en de ernst van de gevolgen van vals positieven worden verstevigd door ontwikkelingen binnen ons materieel strafrecht waarbij gedragingen in een steeds vroeger stadium strafbaar zijn (bijvoorbeeld voorbereidingshandelingen) en deelnemingsvormen steeds ruimer worden geformuleerd (medeplegen, medeplichtigheid).

De problematiek van de vals positieven en vals negatieven kan verduidelijkt worden aan de hand van een simpele afbeelding. De punt van de piramide is een 'traditioneel' delict, bijvoorbeeld een reactief opsporingsonderzoek dat naar aanleiding van een moord wordt gestart. Bij een dergelijk delict is de kring van mogelijke verdachten over het algemeen beperkt. De bodem van de piramide wordt gevormd door een pro-actief

opsporingsonderzoek op basis van aanwijzingen dat een terroristisch misdrijf voorbereid wordt. In dit geval is er nog geen helder zicht op de verdachte(n). Het risico bestaat dus dat een groter aantal mensen wordt meegenomen in het 'sleepnet' van de opsporingsinstanties. Hierdoor wordt de kans op vals positieven aanzienlijk groter. In feite is er dus een verschuiving gaande van 'zekerheden' naar 'waarschijnlijkheden'.



10 Privacy, autonomie en grondrechten

Uit hoofdstuk 6 is reeds besproken dat het recht op privacy en de bescherming van persoonsgegevens vaak naar voren komen in discussies rondom de verhouding tussen veiligheid en grondrechten. Na de bespreking van de toekomstige technologische ontwikkelingen en de mogelijke risico's van toezicht / surveillance is het raadzaam om nogmaals het recht op (informatie) privacy te bekijken.

Zoals aangegeven in hoofdstuk 6 is een eenduidige definitie van het begrip privacy moeilijk tot niet te geven. Wanneer we kijken naar de concepties van het recht op privacy dan zien we dat het recht op privacy voor verschillende doeleinden dient. Het gaat dan onder andere om het beschermen van de persoonlijke autonomie, het afsluiten voor invloeden van buitenaf en het mogelijk maken van sociale interactie.

Wanneer we het recht op privacy beschouwen in relatie tot veiligheidsmaatregelen binnen Secure Haven, dan zien we dat het recht op privacy primair gepositioneerd wordt als een middel om informatie af te scherpen van derden. Doordat effectieve controle is gebaseerd op kennis van het te controleren domein (een persoon, proces of plaats), vermindert het recht op privacy de mogelijkheden tot controle (en daarmee macht). In deze context heeft het recht op privacy primair tot doel de persoonlijke autonomie te waarborgen en de machtsbalans tussen de controleur en de gecontroleerde te waarborgen.

Eenzelfde conclusie kan getrokken worden voor de bescherming van persoonsgegevens (een species van het recht op privacy). Jeroen van den Hoven (2008) geeft vier ethische gronden voor de bescherming van persoonsgegevens te weten: 1) *information-based harm*, 2) *informational inequality*, 3) *informational injustice*, en 4) *moral autonomy and moral identification*.

Het gebruik van persoonsgegevens voor veiligheidsdoeleinden binnen Secure Haven kan de autonomie van personen aantasten (zij zijn immers minder vrij in hun handelen). Daarnaast kan een gebruik van persoonsgegevens buiten de context waarin zij verwerkt zijn leiden tot het trekken van verkeerde conclusies over personen (waardoor *information-based harm* kan ontstaan). Het gevolg hiervan zijn de eerder genoemde vals positieven. Tot op zekere hoogte zouden we dus kunnen stellen dat het recht op privacy naast een op zichzelf staande waarde, binnen Secure Haven ook een middel is om andere belangen zoals de persoonlijke autonomie en grondrechten als de vrijheid van meningsuiting, vrijheid van vergadering en vrijheid van godsdienst te waarborgen.

Een voorbeeld kan deze conclusie illustreren. Wanneer mensen weten dat de politie tijdens een politieke manifestatie binnen Secure Haven demonstranten gaat filmen en vraagt naar hun legitimatie, kan dit betekenen dat zij niet (of niet meer) mee zullen doen met de manifestatie. Dit uit angst dat het vastleggen van hun aanwezigheid mogelijk negatieve consequenties voor hen kan hebben. Het verwerken van persoonsgegevens door de politie zorgt er aldus voor dat mensen niet langer vrij voor hun mening durven uit komen. De schending van de (informatie) privacy van de burgers zorgt er in dit geval voor dat het grondrecht op vrijheid van meningsuiting wordt aangetast. Het recht op privacy (het verbieden om mensen te filmen en zonder reden vragen naar legitimatie) wordt in deze dan ook als middel ingezet om de vrijheid van meningsuiting te waarborgen.

Vergelijkbare voorbeelden zijn aan te halen voor andere grondrechten. Kern van het argument is dat de aanwezigheid of mogelijke aanwezigheid van toezicht een (zelf)disciplinerende werking heeft op de burger. Dit is het panoptische model dat in hoofdstuk 9 is aangehaald. Het recht op privacy zorgt ervoor dat mensen niet gehinderd worden in hun handelen. Aldus beschermt het recht op privacy de persoonlijke autonomie en waarborgt het de vrije uitoefening van de verschillende grondrechten.

11 Grondrechten en veiligheid

Hoewel grondrechten en veiligheid niet met elkaar hoeven te botsen, kunnen zij in bepaalde situaties op gespannen voet met elkaar staan. Gegeven het feit dat het doel van veiligheidsmaatregelen is om meer controle

te krijgen op een proces, persoon of plaats, bestaat de mogelijkheid dat veiligheidsmaatregelen bewust of onbewust negatieve invloed hebben op de grondrechten van de personen die aan de maatregelen onderworpen worden. De vraag is dan hoe de rechten en belangen van het individu zich verhouden tot de rechten en belangen van de maatschappij als geheel. Meestal wordt deze vraag *ex post* beantwoord: aan de hand van een concreet geval toetst de rechter hoe de inzet van een bepaalde veiligheidsmaatregel zich verhoudt tot de grondrechten van het individu.

Het vooraf (*ex ante*) toetsen van veiligheidsmaatregelen aan grondrechten is beduidend lastiger. Er bestaat nu eenmaal geen duidelijk antwoord op de vraag wanneer de belangen tussen het individu enerzijds en de maatschappij anderzijds 'in balans' zijn. Er is dus ook niet zoiets als 'genoeg privacy' of 'afdoende vrijheid'. Uiteindelijk is de keuze voor het al dan niet invoeren van veiligheidsmaatregelen die een (mogelijke) beperking van of bedreiging vormen voor de grondrechten van burgers een politieke keuze. Hierbij dient de politiek af te wegen wat de effectiviteit van de maatregel is (hoeveel veiliger wordt het?) en wat de mogelijke risico's van de maatregel zijn (hoe verhoudt de maatregel zich tot de rechten van de burger?). Deze belangenafweging kan ondersteund worden door het aanreiken van een aantal criteria op basis waarvan we kunnen toetsen of een veiligheidsmaatregel in overeenstemming is met hetgeen wij in onze democratische rechtsstaat acceptabel vinden.

Het is ook van belang dat de afweging niet in belangrijke mate wordt beïnvloedt door het fenomeen van de 'geanticiperde beslissingsspijt' (zie bijv. Tijmstra 2001). Bij het nemen van individuele veiligheidsmaatregelen speelt vooral het feit dat mensen toekomstige spijt door een verkeerd gemaakte keuze willen voorkomen. Dit wordt 'geanticiperde beslissingsspijt' (anticipated decision regret) genoemd. Risico's die verminderd kunnen worden door menselijk ingrijpen krijgen in zo'n situatie meer aandacht dan risico's waarop de menselijke invloed miniem is. Dat kan tot een grote scheefgroei leiden in de verhouding tussen risicovermindering, financiële investering en grondrechten van burgers.

Deze geanticiperde beslissingsspijt ligt in casu vooral bij de overheid. Veiligheid – en dan in het bijzonder beveiliging tegen (terroristische) aanslagen – heeft bijzonder veel aandacht gekregen. Het lijkt erop dat de overheid bereid is veel te investeren om de kans op een aanslag te minimaliseren omdat ze niet de kans wil lopen het verwijt te krijgen dat een aanslag voorkomen had kunnen worden.

11.1 Effectiviteit veiligheidsmaatregelen

Nog voor we toekomen aan een verkenning van de verhouding tussen grondrechten en veiligheidsmaatregelen dient te worden vastgesteld of een voorgenomen veiligheidsmaatregel daadwerkelijk effectief is. Wanneer met het invoeren van de veiligheidsmaatregel niet het beoogde doel van het vergroten van veiligheid en leefbaarheid wordt bereikt, komen we niet eens toe aan het beantwoorden van de vervolgvraag hoe de veiligheidsmaatregel zich dient te verhouden tot de grondrechten van de burger. Deze effectiviteitsvraag is bovenal een vraagstuk van kosten en efficiëntie: hoeveel kost het invoeren van een bepaalde maatregel, hoeveel levert het in termen van veiligheid op, en zijn er alternatieven die beter/effectiever zijn?

In dit kader zullen wij twee problemen schetsen voor de effectiviteit van een veiligheidsmaatregel te weten: 1) information overload en 2) diffuse risico's.

11.1.1 Information overload

Een veelvoorkomende valkuil bij het invoeren van veiligheidsmaatregelen is het grote vertrouwen in de effectiviteit van technologie.²³ Veel hedendaagse veiligheidsmaatregelen zijn gebaseerd op het verzamelen en verwerken van (persoons)gegevens. Deze gegevens worden gebruikt om in te grijpen of te sturen. Echter, het verzamelen van gegevens (data) leidt niet noodzakelijkerwijs tot meer kennis (relevante informatie binnen een bepaalde context die gebruikt kan worden om betere beslissingen te nemen). Bij veel moderne veiligheidsmaatregelen speelt het probleem van 'information overload' (zie hoofdstuk 8). Information overload belemmert de effectiviteit van een veiligheidsmaatregel.

²³ Zie voor een bespreking van deze problematiek onder andere het rapport *Data voor Daadkracht* van het Ministerie van Binnenlandse Zaken.

Een goed voorbeeld van deze problematiek zien we bij de toepassing van beveiligingscamera's. Uit onderzoek naar de toepassing van beveiligingscamera's in Groot Brittannië blijkt dat waarschijnlijk zo'n 80% van het materiaal van de camera's slecht bruikbaar is voor opsporingsdoeleinden (Gerrard, *et al.* 2007). Ook de London Metropolitan Police zelf geeft aan dat de meer dan tienduizend camera's in London niet significant bijdragen aan het oplossen van misdaden. In sommige districten waar weinig camera's hangen is het ophelderingspercentage zelfs hoger dan in districten waar veel camera's hangen.²⁴ De oorzaak hiervoor ligt in de gebrekkige kwaliteit en verwerking van de beelden. Omdat de verwerking van het beeldmateriaal tekortschiet (en daarmee de camera's vaak niet bijdragen aan een hogere pakkans), neemt ook de preventieve werking die van de camera's uitgaat af.

Ook rondom de voorstellen voor het opslaan van verkeersgegevens (dataretentie) bestaan twijfels of de maatregel überhaupt wel effectief is.²⁵

11.1.2 Diffuse risico's

Diffuse risico's, zoals risico's van aanslagen vanuit de georganiseerde misdaad of het terrorisme, zijn moeilijk aan te pakken. De reden hiervoor ligt in het feit dat een crimineel of terrorist een menselijke actor is die zich kan aanpassen aan veranderende omgevingsfactoren en omstandigheden. De aanslagen van 11 september 2001 vormen hiervan een goed voorbeeld. Ongetwijfeld was sinds de eerdere aanslagen in de kelder van het WTC de bewaking verscherpt. Wellicht zou een terrorist die opnieuw een bom in z'n auto die kelder in wilde rijden inderdaad zijn onderschept. Een onverwachte 'nieuwe' vorm van terrorisme schokt dan de wereld, en onmiddellijk worden er maatregelen genomen om *die* vorm van terrorisme voortaan te voorkomen. Met innovatieve terroristen wordt echter te weinig rekening gehouden. Zo leiden veiligheidsmaatregelen vaak tot verandering en/of verplaatsing van risico's, niet noodzakelijkerwijs tot een algehele reductie ervan.

11.2 Eisen vanuit het recht

Wanneer een veiligheidsmaatregel (waarschijnlijk) het beoogde effect kan bereiken, is vervolgens de vraag in hoeverre het veiligheidsbelang te verenigen is met de grondrechten van de burger. Wanneer deze niet (goed) met elkaar te verenigen zijn is de vraag welke van de twee belangen in concreto zwaarder dient te wegen.

Bij de beantwoording van deze vraag kunnen we ons laten leiden door een aantal toetsingscriteria uit de wet en de literatuur. Een voor Nederland belangrijke (zo niet de belangrijkste) toetssteen hierbij is het Europees Verdrag voor de Rechten van de Mens.

Het Europees Verdrag voor de Rechten van de Mens (EVRM) waarborgt de grondrechten van de Europese burger. Deze grondrechten zijn echter niet absoluut en kunnen dus onder bepaalde voorwaarden beperkt worden. Dergelijke beperkingen moeten wel aan de eisen van de democratische rechtsstaat voldoen. Een goed voorbeeld van hoe deze eisen gecodificeerd zijn zien we in artikel 8 EVRM:²⁶

"1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

Uit lid 2 van artikel 8 EVRM kunnen we opmaken dat veiligheidsmaatregelen die in het kader van het Secure Haven programma ingevoerd worden moeten voldoen aan minimaal de volgende eisen: zij moeten 1) bij de wet voorzien zijn en 2) noodzakelijk zijn in een democratische samenleving.

²⁴ <http://www.guardian.co.uk/uk/2008/may/06/ukcrime1>

²⁵ Zie bijvoorbeeld: Van den Berg, A. IJ. (2008), Dataretentie helpt nauwelijks, in: *NRC Handelsblad*, 10 april 2008

²⁶ Hetgeen hier specifiek over het recht op privacy wordt gezegd (artikel 8 EVRM) geldt ook voor andere grondrechten zoals het recht op vrijheid van meningsuiting, omdat in de betreffende artikelen dezelfde eisen aan beperkingen op het grondrecht worden gesteld.

Deze eisen vormen een goed vertrekpunt bij de beoordeling of een veiligheidsmaatregel in overeenstemming is met de eisen die daaraan gesteld mogen worden in een democratische rechtsstaat. Hieronder zullen deze en andere toetsingscriteria nader verkend worden.

11.2.1 Bij de wet voorzien

Allereerst moet een inbreuk op het grondrecht bij de wet voorzien zijn en dus gebaseerd zijn op een wettelijke bevoegdheid. Deze wettelijke bevoegdheid moet voldoende duidelijk en toegankelijk zijn voor de burger. Met andere woorden de wettelijke bepaling moet voldoende duidelijk geformuleerd en afgebakend zijn (kwaliteit van de wet) en ook voor de burger kenbaar zijn (transparantie).

11.2.2 Noodzakelijk in een democratische samenleving

Ten tweede moet de inbreuk op het grondrecht noodzakelijk zijn in een democratische samenleving. Dit betekent dat er allereerst een legitiem doel mee moet worden nagestreefd (de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen).

Uit de noodzakelijkheid vloeit ook voort dat de inbreuk in verhouding moet staan tot het na te streven doel en dat er geen minder ingrijpend middel beschikbaar is. Het gaat hier dus om een *proportionaliteits-* en een *subsidiariteitseis*.

Bij de toetsing van de proportionaliteit moet gekeken worden hoe de veiligheidsmaatregel zich verhoudt tot de rechten van de burger. De afweging die gemaakt moet worden is die tussen de invloed van de maatregel op de grondrechten van de burger (hoe ernstig is de inbreuk) en de mate waarin de maatregel bijdraagt aan het belang dat met de maatregel wordt nagestreefd (in concreto veiligheid). De vraag die bij de proportionaliteitstoets gesteld moet worden is: *rechtvaardigt de te verwachten bijdrage van de maatregel aan de veiligheid de voorziene inbreuk op de grondrechten van het individu?*

Bij de subsidiariteitstoets wordt gekeken of er geen minder ingrijpende maatregelen zijn die het nagestreefde belang net zo goed kunnen beschermen. Wanneer deze voorhanden zijn is het niet toegestaan het zwaardere middel in te zetten. Bij het nemen van veiligheidsmaatregelen moet dus altijd worden uit gegaan van een 'minimum-aanpak'. Met andere woorden: je mag niet met een kanon op een mug schieten.

11.3 Toetsingscriteria verhouding veiligheid en grondrechten

De wettelijke eisen die voortvloeien uit het EVRM kunnen nader concreet worden gemaakt aan de hand van diverse toetsingscriteria. In deze paragraaf zullen een aantal van deze criteria worden besproken.

11.3.1 Beïnvloeding bestaande machtsverhoudingen

Veiligheidsmaatregelen vergroten de mate van controle die degene die de maatregelen beheerst kan uitoefenen. Dit idee komt voort uit het aloude adagium van Sir Francis Bacon (1597): "*kennis is macht.*" Hoe meer iemand weet over een persoon, plaats, en/of proces hoe beter hij in staat is om te sturen en te controleren. Ook de enkele suggestie van aanwezige controle kan voldoende zijn om een gedragsverandering in personen te bewerkstelligen (zie voor een verdere bespreking van deze problematiek de volgende paragraaf).

Bij de invoering van veiligheidsmaatregelen is het dus zaak te bekijken in hoeverre veiligheidsmaatregelen de bestaande machtsverhoudingen tussen burgers en overheid beïnvloeden.²⁷ Wanneer een maatregel de machtsverhouding (verder) in het voordeel van de overheid doet doorslaan, past terughoudendheid bij de toepassing daarvan. Het is hierbij van belang veiligheidsmaatregelen niet als op zichzelf staand te beschouwen, maar te beoordelen in hun onderlinge samenhang.

11.3.2 Beïnvloeding gedrag burgers

In samenhang met hetgeen in de vorige paragraaf is gezegd over verschuivende machtsverhoudingen ligt de beïnvloeding van de burger. Wanneer een burger weet dat hij in de gaten gehouden wordt (of kan worden)

²⁷ Een vergelijkbare analyse kan gemaakt worden bij de toepassing van controle- en toezichtmethoden in de verhouding bedrijfsleven-burger en burger-burger.

dan bestaat de kans dat deze zijn gedrag gaat aanpassen aan de heersende norm om aldus niet in negatieve zin op te vallen (Foucault, 1995). Wanneer een burger bijvoorbeeld weet dat hij zijn identiteit niet kan verbergen voor het heersende gezag als hij een zeer uitgesproken of radicale politieke mening uit, dan bestaat de kans dat deze burger minder of in het geheel niet die mening uit. Een dergelijke houding die wordt ingegeven door de controle mogelijkheden van de overheid verstart het democratisch proces en is in strijd met de vrijheid van meningsuiting.

Het is daarom bij veiligheidsmaatregelen van belang een inschatting te maken hoe deze het gedrag van de burger mogelijk beïnvloeden en of een dergelijke ‘gedwongen’ gedragsverandering wenselijk en legitiem is.

11.3.3 Mogelijkheden tot misbruik

Hoewel veiligheidsmaatregelen tot doel hebben de veiligheid en leefbaarheid te vergroten, kunnen zij op zichzelf ook een risico vormen. Dit geldt zowel voor het misbruik van bevoegdheden door de overheid (het Big Brother scenario) als het gebruik door kwaadwillende derden (criminelen, kwaadwillende hackers en dergelijke). Bij de beoordeling van de wenselijkheid van een veiligheidsmaatregelen dienen deze mogelijkheden tot misbruik nadrukkelijk meegewogen te worden.

11.3.4 Checks and balances

Een zeer belangrijk element bij de beoordeling hoe een veiligheidsmaatregel zich verhoudt tot de grondrechten van het individu zijn de waarborgen (checks and balances) waarmee de veiligheidsmaatregel omgeven is. Een algemene stelregel is dat naarmate de bevoegdheid of de maatregel meer risico's met zich meebrengt voor de grondrechten van de burger, deze omgeven dient te worden met meer waarborgen.

Deze waarborgen kunnen op diverse manieren gestalte krijgen en hebben onder andere betrekking op de procedures waarmee de toepassing van een maatregel is omkleed, de wijze waarop bezwaar kan worden gemaakt tegen de toepassing ervan en de controle die er is op het gebruik en de inzet van de maatregel/bevoegdheid.

11.3.5 Transparantie

Uit het EVRM komt reeds naar voren dat inbreuken op grondrechten bij de wet moeten zijn voorzien en dat deze wetgeving voldoende duidelijk en toegankelijk moet zijn. Naast de invulling van deze eis per veiligheidsmaatregel is het ook van belang hoe de maatregelen zich onderling tot elkaar verhouden en wie de instanties zijn die de bevoegdheden hebben tot het uitoefenen van veiligheidsmaatregelen.

11.3.6 Informatieele zelfbeschikking

Het recht op informatiele privacy zoals geformuleerd door Westin (1967) geeft aan dat een individu zelf kan bepalen wat er met zijn of haar persoonlijke informatie gebeurt. Uit deze formulering kan het beginsel afgeleid worden dat binnen de relatie overheid - burger, de burger zelf mag bepalen in hoeverre informatie over hem of haar wordt gebruikt. Dit wordt ook wel *informatieele zelfbeschikking* genoemd. Dit recht op informatiele zelfbeschikking is niet absoluut: zoals meerdere malen naar voren is gekomen in deze rapportage moet de burger zich bepaalde beperkingen op zijn of haar grondrechten laten welgevalen. De Nederlandse wetgever heeft in de Memorie van Toelichting bij de Wet bescherming persoonsgegevens aangegeven dat het recht op informatiele zelfbeschikking, buiten de werkingssfeer van artikel 10, eerste lid, als zodanig geen onderdeel uitmaakt van de Nederlandse rechtsorde.²⁸ Als algemeen uitgangspunt geldt dat noch de handelingsvrijheid van de degene die persoonsgegevens verwerkt, noch het recht op bescherming van de persoonlijke levenssfeer van de betrokkene in abstracto zwaarder weegt. Als in een concreet geval beide belangen dreigen te botsen, dienen zij tegen elkaar te worden afgewogen, waarbij rekening moet worden gehouden met de bijzondere (grondwettelijke) waarde van het recht op bescherming van de persoonlijke levenssfeer.²⁹

Hoewel er in Nederland als zodanig dus geen volledig recht op informatiele zelfbeschikking is, is het zinvol en wenselijk om de burger waar mogelijk naast inzicht (transparantie) ook inspraak te geven in de verwerking van zijn of haar gegevens (een recht op inzage, verbetering en wellicht zelfs afscherming). Naast het

²⁸ Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3, p. 9

²⁹ Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3, p. 9

feit dat de burger meer controle krijgt over het gebruik van zijn of haar gegevens, waardoor de machtsbalans tussen overheid en burger beter gewaarborgd blijft, kan zelfbeschikking ook bijdragen aan een betere gegevensverwerking en acceptatie van veiligheidsmaatregelen.

12 Oplossingsrichtingen

Zoals eerder aangegeven is de keuze voor het nemen van een bepaalde veiligheidsmaatregel primair politiek van aard. Aan de hand van de in deze rapportage opgesomde risico's en de relevante toetsingscriteria, dient een afgewogen beslissing te worden genomen over het al dan niet nemen van een bepaalde veiligheidsmaatregel.

De keuze voor het nemen van een veiligheidsmaatregel impliceert niet per definitie dat daarmee grondrechten van ondergeschikt belang zijn. Veiligheid en grondrechten worden vaak als tegengestelde belangen gepositioneerd, maar dit is een valse tegenstelling. Veiligheid en grondrechten zijn belangen die beiden maximaal nagestreefd dienen te worden. Desalniettemin kunnen beide belangen soms moeilijk met elkaar te verenigen zijn.

Om het veiligheidsbelang en het belang van individuele grondrechten beide te dienen zijn een aantal oplossingsrichtingen aanwezig. Hieronder schuiven wij een aantal mogelijke oplossingen naar voren die moeten bijdragen aan het verenigen van de verschillende belangen.

12.1 Democratische legitimatie en borging

Een noodzakelijke voorwaarde voor de invoering van veiligheidsmaatregelen is de democratische legitimatie. Dit betekent allereerst dat de invoering van veiligheidsmaatregelen overeen moet komen met de eisen zoals vastgelegd in de internationale verdragen en nationale wetten (zie hoofdstuk 7). Deze toetsing is de verantwoordelijkheid van de Eerste en Tweede Kamer. Rechterlijke toetsing van wetten en maatregelen wordt in belangrijke mate beperkt door het verbod op grondwettelijke toetsing. Wel kan de rechter in concrete gevallen aangeven of de toepassing van een bevoegdheid of maatregel in strijd is met bepaalde grondrechten.

Naast de parlementaire toetsing vindt toetsing van concrete maatregelen plaats via het Ministerie van Justitie, het Ministerie van Binnenlandse Zaken en het Openbaar Ministerie. Het toezicht ligt voornamelijk bij het College bescherming persoonsgegevens.

Op gemeentelijk niveau (relevant voor Secure Haven) is het naast het College de Gemeenteraad die moet toezien op een zorgvuldige belangenafweging tussen veiligheid en grondrechten.

12.1.1 Burgerparticipatie

Om de democratische legitimatie van veiligheidsmaatregelen te vergroten binnen Secure Haven dient de burger betrokken te worden bij de invoering en het gebruik van veiligheidsmaatregelen. Dit betekent naast inspraak bij de invoering van veiligheidsmaatregelen ook mogelijkheden om inzicht in de werking te krijgen via voorlichting en periodieke toetsing. Een dergelijke aanpak zal naar alle waarschijnlijkheid ook de acceptatie van de maatregelen door de burgers van Secure Haven vergroten.

12.2 Periodieke toetsing

Om de democratische legitimatie van veiligheidsmaatregelen blijvend te garanderen dient de toepassing ervan periodiek getoetst te worden. Voornaamste beoordelingscriteria zijn de effectiviteit van een maatregel en de invloed ervan op de burger. Daarnaast kan gekeken worden of er sinds de introductie van een maatregel niet betere en minder privacygevoelige methoden en technieken zijn geïntroduceerd.

12.3 Limitering duur veiligheidsmaatregelen

Strengere veiligheidsmaatregelen passen bij een hoog dreigingsniveau en/of een groot veiligheidsrisico. Wanneer een veiligheidsrisico naar verloop van tijd afneemt of een acute dreiging verdwijnt, past ook een minder streng veiligheidsregime. In het verlengde van een periodieke toetsing zou een limitering op de duur van een veiligheidsmaatregel dus ook een mogelijkheid bieden om de inbreuk op de grondrechten te beperken.

12.4 Voorkomen systeemdwang

Veel veiligheidsmaatregelen, in bijzonder die met een sterke ICT-component, hebben de neiging alomvatkend te zijn. Met andere woorden, het systeem laat geen ruimte meer voor alternatieve handelwijzen. Bij

dergelijke maatregelen is er sprake van ‘systeemdwang’. Hierdoor wordt de burger gedwongen deel te nemen aan het systeem en de keuzes die het biedt. Om deze reden worden dergelijke maatregelen ook wel ‘virtuele dwangbuizen’ genoemd (Mommers 2008). Bij veel veiligheidsmaatregelen is dit ook een noodzakelijke voorwaarde voor de werking ervan (een toegangscontrole bijvoorbeeld die je kan omzeilen is niet zo zinvol). Echter, systeemdwang kan een inbreuk zijn op de autonomie van het individu. In de meeste gevallen zullen burgers zich schikken naar hun lot en zich aanpassen aan het systeem, maar waar die aanpassing ongewenst is, moet naar alternatieven worden gezocht.

Bij het toepassen van ICT in het kader van veiligheid moet dus in het bijzonder voor de valkuil van virtuele dwangbuizen worden gewaakt. Dit is met name het geval wanneer het systeem eisen stelt aan de burger die niet noodzakelijkerwijs bijdragen aan het bewerkstelligen van het nagestreefde veiligheidsdoel. Bij de beoordeling van de ernst van systeemdwang spelen de eisen van subsidiariteit en proportionaliteit dan ook een belangrijke rol.

12.5 Privacy by design

Wet- en regelgeving vormen noodzakelijke voorwaarden voor de zorgvuldige toepassing van veiligheidsmaatregelen. Echter, wetten op zichzelf bieden niet direct concrete en effectieve bescherming. Vaak zijn wetten ‘vaag’ door hun open normstelling en bieden voor de praktijk niet de noodzakelijke concrete handvatten. Ook bestaat de mogelijkheid dat door bijvoorbeeld onbekendheid of onzorgvuldigheid, de wettelijke vereisten die bij de toepassing van veiligheidsmaatregelen in acht genomen dienen te worden niet nageleefd worden.

De inrichting van een veiligheidsmaatregel in zowel procedurele/organisatorische zin als in technische zin bepaalt uiteindelijk hoe ‘privacygevoelig’ deze is. Door veiligheidsmaatregelen en technologieën op dusdanige wijze te ontwerpen en te implementeren dat zij een minimale inbreuk op de privacy (en andere grondrechten) bewerkstelligen kunnen wetten en regels veel effectiever worden nageleefd. Door bijvoorbeeld in de software vast te leggen dat gegevens niet langer dan 24 uur worden bewaard, kunnen veel privacyrisico’s worden vermeden. Een dergelijke benadering noemen we ‘privacy by design’. Privacy by design vraagt een multi-disciplinaire aanpak waarbij technici, juristen, sociologen en bestuurders gezamenlijk komen tot de functionele en technische vereisten voor veiligheidsmaatregelen.

Het principe van privacy by design dient het vertrekpunt te zijn bij de introductie van veiligheidsmaatregelen binnen Secure Haven.

12.5.1 Minimalisatie en anonimisering

Bij de toepassing van veiligheidsmaatregelen waarbij persoonsgegevens worden verwerkt dienen minimalisatie en anonimisering van gegevens het uitgangspunt te zijn. Deze ontwerpdoelstellingen vloeien voort uit de wet en de eisen van proportionaliteit en subsidiariteit (zie ook de paragraaf over systeemdwang). Hoewel voor de werking van veiligheidsmaatregelen zoals toegangscontrole en toezicht de verwerking van persoonsgegevens noodzakelijk kan zijn, dient deze gegevensverwerking zich altijd tot het minimaal noodzakelijke te beperken. Naast minimalisatie is ook anonimisering van belang. Veelal is identificatie van personen niet noodzakelijk voor de goede werking van het systeem. Anonieme verwerkingen verdienen in dergelijke gevallen de voorkeur.

Dataminimalisatie en anonimisering kunnen software- en hardwarematig worden ingebouwd in het systeem (zie vorige paragraaf). Daarnaast dienen ook procedurele stappen te worden genomen om waar mogelijk minimalisatie en anonimisering te bewerkstelligen.

Het minimaliseren en anonimiseren van gegevensverwerkingen is niet alleen van belang met het oog op de privacy van de burger. Grote hoeveelheden (nodeloos) opgeslagen (persoons)gegevens vormen namelijk op zichzelf ook weer een veiligheidsrisico. Bijvoorbeeld wanneer deze gegevens in handen komen van kwaadwillende derden.

13 Conclusie

Het garanderen van veiligheid is een van de kerntaken van de overheid. De overheid mag maatregelen nemen om de veiligheid te vergroten of te verbeteren, zelfs als dit een potentiële inbreuk op de autonomie van de burger betekent. Echter, de overheid dient terughoudend te zijn bij het nemen van veiligheidsmaatregelen die een inbreuk kunnen vormen op de grondrechten van de burger. Op basis van deze uitgangspunten werd de volgende probleemstelling geformuleerd:

Hoe kunnen veiligheid en respect voor grondrechten tegelijkertijd optimaal gewaarborgd worden binnen Secure Haven?

Wat uit deze rapportage naar voren komt is dat een eenduidig antwoord op deze probleemstelling eigenlijk niet goed mogelijk is, omdat er nu eenmaal geen heldere balans bestaat tussen veiligheid en grondrechten. Dit is enerzijds omdat grondrechten en veiligheid geen grootheden zijn die tegen elkaar uitgewisseld kunnen worden en anderzijds omdat er geen duidelijk punt op een schaal is waar er sprake is van 'genoeg veiligheid' of 'genoeg respect voor grondrechten'. Uiteindelijk blijft de keuze voor het invoeren van veiligheidsmaatregelen die op gespannen staan met de grondrechten van het individu een politieke keuze.

Bij deze keuze wordt een afweging gemaakt tussen de belangen van de maatschappij als geheel (veiligheid) en de individuele rechten van de burger. Naast de toetsing van de effectiviteit van een maatregel vormt het juridisch toetsingskader zoals uiteengezet in hoofdstuk 11 de voornaamste leidraad voor een beoordeling of een veiligheidsmaatregel al dan niet ingevoerd dient te worden. Overigens moet bij de invoering van veiligheidsmaatregelen, voornamelijk daar waar het gaat om opsporingsbevoegdheden, de zelfstandige bevoegdheid van de gemeente Den Haag niet overschat worden.

Het is van belang dat de afweging tussen veiligheid en grondrechten breder wordt getrokken dan het collectief tegenover het individu. Veiligheidsmaatregelen beïnvloeden niet alleen de rechten van het individu, maar hebben ook hun effect op de maatschappij als geheel. Mogelijke risico's van veiligheidsmaatregelen zijn uiteengezet in hoofdstuk 9. Bij de politieke keuze dient dus niet alleen rekening te worden gehouden met de mogelijke risico's die veiligheidsmaatregelen kunnen voortbrengen voor het individu, maar ook voor de samenleving als geheel. Hierbij dienen veiligheidsmaatregelen in hun onderlinge samenhang bekeken te worden. Voor Secure Haven betekent dit dat goed gekeken moet worden hoe veiligheidsmaatregelen burgers en bezoekers raken, welke gevoelens burgers hierbij hebben, en hoe dit het leven binnen de gemeente Den Haag en de Internationale Zone beïnvloedt.

Wanneer uiteindelijk wordt besloten tot de invoering van bepaalde veiligheidsmaatregelen waarbij een risico bestaat voor de grondrechten van de burger, dan kan via de in hoofdstuk 12 genoemde oplossingsrichtingen getracht worden de risico's te minimaliseren.

14 Aanbevelingen

Op basis van de conclusies uit deze rapportage worden de volgende aanbevelingen gedaan vanuit werkpakket 1120:

- Bij de introductie van veiligheidsmaatregelen wordt vaak onvoldoende stil gestaan bij de effectiviteit van de maatregel. Het verdient de voorkeur om voor de introductie van een nieuwe veiligheidsmaatregel een beter beeld te krijgen van de te verwachten effectiviteit. Mogelijke aanknopingspunten voor een dergelijke analyse zijn met name ‘best and bad practices’ uit andere steden.
- Het verdient de voorkeur om voor de invoering van veiligheidsmaatregelen een ‘impact assessment’ te doen waarin gekeken wordt wat de invloed van de maatregel is op de grondrechten van de burger. Voor een dergelijke assessment kan het toetsingskader uit deze rapportage worden gebruikt alsmede best-and-bad practices uit andere steden.
- Veiligheidsmaatregelen dienen niet op zichzelf, maar in samenhang te worden beschouwd. Bij de toetsing van de invloed die veiligheidsmaatregelen hebben op de grondrechten van burgers dient het totale pakket aan veiligheidsmaatregelen te worden getoetst.
- Er dient aanvullend onderzoek te worden gedaan naar de veiligheidsbeleving van burgers binnen Secure Haven om te kijken in hoeverre burgers zich veiliger of onveiliger (big brother is watching you) voelen door de introductie van nieuwe veiligheidsmaatregelen.
- Veiligheidsmaatregelen binnen Secure Haven dienen ontworpen te worden via de principes van ‘privacy by design’ en naarmate de risico’s voor grondrechten toenemen, omkleed te worden met waarborgen zoals uiteengezet in hoofdstuk 11 en 12.

15 Verkorte bibliografie

- Aarts, E., Harwig, R., Schuurmans, M. (2002). *Ambient Intelligence*, in: Denning, P.J. (ed.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, pp. 235-250. New York: McGraw Hill
- Bacon, F. (1597). *Magna Instaurationis*.
- Bentham, J. (1843). *Jeremy Bentham: Collected Works*. (J. Browning, Red.) London.
- Berlin, I. (1958). *Two concepts of Liberty*, opnieuw uitgebracht in 2002 als: *Liberty* (red. Hardy, H.), Oxford: Oxford University Press
- Blok, P. (2002). *Het Recht op Privacy*. Den Haag: Boom Juridische Uitgevers.
- Cleiren, C. P. (2006). 'Aanwijzingen' voor de wetgeving bij veiligheidsvraagstukken en terrorismebestrijding. In e. a. W. Huisman, *Veiligheid en Recht*. Den Haag: Boom Juridische Uitgevers.
- Dubbeld, L. (2004). *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance*. Enschede: Ipskamp Printpartners.
- Gerrard, G. et al. (2007), *The National CCTV Strategy*, UK Home Office, oktober 2007
- Foucault, M. (1995). *Discipline and Punish, the Birth of the Prison*. New York: Vintage Books.
- Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*. Amsterdam: Otto Cramwinkel.
- Kean, T.H. et al. (2004), *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks on the United States*, official government edition, US Government Printing Office
- Nieuwenhuis, A. J. (2001). *Tussen Privacy en Persoonlijkheidsrecht, een grondrechtelijke en rechtsvergelijkend onderzoek*. Nijmegen: Ars Aequi Libri.
- Mommers, L. (2008). Virtuele dwangbuizen en controleneurose, in: *Tijdschrift voor Internetrecht*, nummer 1 maart 2008.
- Poster, M. (1990). *The Mode of Information*. Cambridge: Polity Press.
- Roosevelt, F. D. R. (1941), *Annual Address to Congress 'the Four Freedoms'*, 6 januari 1941
- Rotenberg, M. (2003). *The Privacy Law Sourcebook 2003*, Washington: Electronic Privacy Information Center.
- Schermer, B. W. (2007). *Software Agents, Surveillance, and Privacy: a Legislative Framework for Agent-Enabled Surveillance*. Leiden: Leiden University Press.
- Schermer, B. W. (2008). *Ambient intelligence, persoonsgegevens en consumentenbescherming*, ECP.NL, mei 2008.
- Smeets, A. H. (2004). *Camera's in het publieke domein. Privacynormen voor eht cameratoezicht op de openbare orde*. College Bescherming Persoonsgegevens. Den Haag: College Bescherming Persoonsgegevens.
- Stichting Nationaal Comité 4 en 5 mei (2007), *Nationaal Vrijheidsonderzoek 2007*.
- Van den Hoven, J. (2008), *Information Technology and Moral Philosophy*, Cambridge University Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy: the Implicit Made Explicit. *Harvard Law Review*, 193-220.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum Press.

16 Appendix

16.1 Scenario's³⁰

Hieronder zijn een drietal scenario's opgenomen welke een concreter beeld geven van hoe de veiligheidsmaatregelen binnen Secure Haven gestalte kunnen krijgen en welke invloed dit (mogelijk) heeft op bewoners en bezoekers. In het tweede deel van de rapportage van WP 1120 zullen deze scenario's getoetst worden via de methode van het Legal Requirements Engineering.

16.1.1 Casus Secure Convention Center district

Locatie: Secure Haven, Datum: 6 februari 2016

Eva Dam en haar man Anton wonen net binnen de grenzen van het gebied dat de gemeente Den Haag al geruime tijd geleden heeft aangewezen als "Secure Haven". Een concept wat de gemeente sindsdien druk aan het implementeren is. Eva werkt normaalgesproken buiten de Randstad, maar vandaag moet ze naar het gloednieuwe congrescentrum in het hart van Secure Haven. Recentelijk heeft de gemeente het congrescentrum en het hele gebied eromheen flink aangepakt. Dat deel van de stad is nu zodanig ingericht, dat de gerichte verkeersstromen door Secure Haven heen onbelemmerd zijn en volledig buiten het "congresgebied" om gaan. De gemiddelde bewoner en forens heeft dus nergens last van. Slechts de mensen die daadwerkelijk in het congresgebied moeten zijn, hoeven zich daarbinnen te begeven.

"En dat is maar goed ook", denkt Eva bij zichzelf terwijl ze haar auto door de nieuwe straten stuurt. Want sinds kort is er weer wat nieuws bedacht: iedereen die het congresgebied betreedt, moet zich laten registreren. Volgens de brochure die Anton en zij van de gemeente hebben gekregen, heeft de maatregel vooral tot doel de overlast en criminaliteit in het voor Secure Haven vitale gebied tot een absoluut minimum te beperken. Anton, die bij het congrescentrum werkt op de nieuwe afdeling 'International conventions acquisitions', baalde behoorlijk. Hij zag het alweer gebeuren, elke ochtend in de rij met alle andere collega's bij Checkpoint Charlie. Gelukkig bleek de gemeente daar wat op bedacht te hebben: mensen die werkzaam zijn binnen het congresgebied krijgen een ID-card, waarmee ze door de geautomatiseerde doorgangen kunnen. En omdat het RFID-technologie betreft kan hij met zijn auto gewoon door de poort rijden, zonder noemenswaardig oponthoud.

Anton werkt veel samen met stafleden van de Internationale Organisaties die zich ook in het gebied bevinden, zoals de UN Criminal Detention Organization, en heeft van die kant ook veel positieve reacties gehoord. Lekker veilig, was de consensus daar. Wel bleek dat de stafleden een anonieme toegangkaart hadden ontvangen. Van hen werd dus alleen geregistreerd dat een geautoriseerd persoon binnenkwam en niet specifiek wie dat was.

"Nee, dan de 'mindere' mensen", denkt Eva opstandig. Ze kent de verhalen al van vrienden. Eerst aanmelden bij de portier van één van de bezoekersingangen, daar registreren door middel van identiteitsbewijs, kenteken registreren en nog wat formaliteiten (biometrie is de bedoeling, maar nu waren er nog wat problemen met de beveiliging van de chips en betrouwbaarheid van de aflezers ofzo). En dan maar hopen dat de rij auto's voor je een beetje doorrijdt. Wat dat betreft gaat het bij de "bezoekerspoort" van het congresgebied, voor de voetgangers, een stuk sneller. Ze heeft trouwens wel gelezen dat je, net zoals de werknemers in het gebied, een persoonsgebonden toegangsabonnement kan aanschaffen. Voor als je vaak wil wandelen door het – toegegeven: prachtig opgeknapt en mooi groene – congresgebied. "Eigenlijk wel leuk en veilig voor de kinderen", denkt ze bij zichzelf.

Voordeel is ook wel dat je niet ergens aangemeld hoeft te zijn of een bepaald doel moet hebben om het gebied in te gaan. Iedereen mag erin, zolang ze zich maar registreren. Eva kan zich de discussies op het digitale

³⁰ Casuïstiek ten behoeve van eerste concretisering Secure Haven – maatregelen, Dikker Hupkes, S., februari 2008

Secure Haven-forum nog levendig herinneren. Mensen op hun achterste benen omdat ‘de toegang tot de publieke ruimte ingeperkt werd’.

Eva vond het ook wel vreemd, dat zo’n groot gebied om een congrescentrum heen met toegangspoorten werd uitgerust maar was allang blij dat er vooralsnog geen bodyscan is neergezet. En volgens de Secure Haven-wethouder bleef het congresgebied gewoon een voor iedereen toegankelijke publieke ruimte. Je hoefde alleen maar even te laten weten wie er nou eigenlijk dat gebied binnenkwam. Ons kent ons in de internationale zone...

De laatste ontwikkeling is de City Sentry, een soort onbemand robotvliegtuig dat permanent boven de stad hangt. Wanneer je een Sentry Pas aanvraagt hoef je je nergens meer te laten registreren. Door de koppeling van diverse technologieën kan de City Sentry je namelijk overal volgen. Wel handig dat je je nooit meer hoeft te laten registreren (en de kinderen raken ook nooit meer zoek) denkt Eva, maar ook wel een onprettig idee dat je altijd en overal te volgen bent.

En ondertussen komt ook haar man aan bij de werknemerspoort even verderop. En terwijl Anton zijn auto door de poort navigeert en hij nog net op het scherm erboven ziet verschijnen “Burger A. Dam, binnenkomst 9 uur 15”, en Eva haar paspoort afgeeft aan de beveiligingsbeambte, denken ze allebei bij zichzelf: “hoe zou dit nou juridisch zitten?”

16.1.2 Casus Congresgebied

Locatie: Secure Haven, hoofdkantoor projectontwikkeling, Stadsdeel Secure Haven, Datum: 6 februari 2018

Sinds het congresgebied in Secure Haven flink op de schop is genomen, is er ook ruimte gecreëerd voor een prestigieus nieuwbouwproject in het kustgebied van Secure Haven. Hier wordt door een combinatie van publieke en private partijen een aantal lage woontorens gebouwd, met daarin mooie – en dure – appartementen voor de “nieuwe bewoners” van Secure Haven. Johan van der Gracht is een ‘young urban professional’ die werkzaam is als PR-medewerker bij een Nederlands bedrijf. Hij zou graag aan het werk gaan bij één van de Internationale Organisaties in Den Haag, zoals bijvoorbeeld de International Seabed Authority, en is dan ook druk bezig met solliciteren. Met die baan in zijn achterhoofd wil hij alvast intekenen voor de nieuwbouwapartementen aan de zee.

Maar helaas wacht hem een akelige verrassing. Bij het kantoor van de projectontwikkelaars bleek tijdens een intakegesprek dat er aan bepaalde vereisten voldaan moest worden voordat je op de wachtlijst kon komen. Wat is namelijk het geval: het dagelijks bestuur van Secure Haven heeft in samenspraak met de gemeente bepaald dat er alleen mensen mogen wonen in het nieuwbouwproject die van bewezen onbesproken gedrag zijn. Het idee erachter is, volgens de medewerker van het kantoor, dat alle bewoners van een bepaald minimumniveau moeten zijn in dit, voor de uitstraling van Secure Haven vitale, woongebied.

Op Johan’s opmerking dat hij nooit iets fout heeft gedaan en erg goed opgevoed is, kwam de reactie dat dit vast zo is, maar wel bewezen moest worden.

Hoewel Johan een door Justitie verleende Verklaring omtrent Gedrag (VOG) kon overleggen waaruit bleek dat hij niet veroordeeld is voor het plegen van strafbare feiten, scoorde hij toch relatief hoog op de risicoschaal van de Secure Haven Autoriteit.

Zo bleek uit het Elektronisch Kinddossier van Johan dat hij op de middelbare school in een aantal vechtpartijtjes was beland. Op basis van dit scoringscriterium kreeg de Secure Haven Autoriteit toegang tot de Nationale DNA Databank om het DNA profiel van Johan te raadplegen (een bevoegdheid die voortvloeit uit de Wet Voorkoming van Gewelddsmisdrijven, Staatsblad, nr. 216, 2014). Uit Johan’s profiel kwam naar voren dat hij positief testte op de aanwezigheid van het pas ongedekte ‘gewelddsgen’.

Verder had de standaard internetscan van Johan een aantal bezwarende Youtube filmpjes opgeleverd waar Johan op een feestje in kennelijk beschonken toestand aan het oreren was dat als hij de macht in Nederland zou hebben het allemaal heel anders geregeld zou worden.

De ambtenaar van de afdeling projectontwikkeling legde Johan uit dat hij op basis van deze informatie Johan een hogere risico waardering had gekregen en hij daarom wel wat uit te leggen had voordat hij Secure Haven binnenkwam.

Zouden die jeugdzondes en dat stomme ‘gewelds gen’ hem nu alle kansen op de nieuwbouwwoning aan het strand kosten? Nee, volgens de medewerker was een bijkomend doel van het project dat er zoveel mogelijk ‘geprivilegieerden’ (stafleden van Internationale Organisaties en hun families) kwamen te wonen. Om dat te promoten, gold voor hen slechts de eis dat ze daadwerkelijk als geprivilegieerde bij het Ministerie van Buitenlandse Zaken geregistreerd stonden. Vervolgens kregen ze voorrang bij de toekenning van woonruimte. Johan van der Gracht begreep dat het nu wel heel belangrijk was dat hij die baan zou krijgen bij de Seabed Authority...

16.1.3 Casus Secure City Manager

Locatie: Secure Haven, Stadsdeel Secure Haven, Datum: 6 februari 2018

Sinds januari 2015 is binnen de internationale zone het project ‘Secure City Manager’ van start gegaan dat tot doel heeft burgers nauwer te betrekken bij de veiligheid en leefbaarheid van hun woonwijk. Hiertoe worden burgers aangesteld als zogenaamde ‘City Managers’.

Speciaal geselecteerde, capabele burgers worden ingezet om de sociale cohesie en controle te bevorderen in de woonwijken van Secure Haven. Het idee hierachter is dat door grote(re) betrokkenheid van burgers (c.q. de bewoners van Secure Haven), de sociale cohesie in een bepaalde wijk zal toenemen. Door toename van de sociale cohesie zal ook de sociale controle toenemen, waardoor de overlast zal afnemen. Het ambt van City Manager is dus eigenlijk tweeledig: 1) het zorgt voor een hechtere band in de gemeenschap, en 2) het draagt bij aan de afname van kleine criminaliteit en overlast.

City Managers doorlopen een selectietraject en krijgen daarna de basiscursus Secure City. Vervolgens wordt de City Manager officieel aangesteld door de gemeente Den Haag. Het betreft hier geen (volledig) bezoldigde functie, maar een functie naast het dagelijks bestaan van de burger. De City Manager is dus officieel werkzaam voor de gemeente, maar blijft vooral inwoner van Secure Haven. De City Manager is het eerste aanspreekpunt van de gemeente in de wijk. Vragen over de gemeente, zoeken naar contacten binnen de gemeente, klachtenregistratie over de gemeente, al deze laagdrempelige vormen van contact met de gemeente verlopen via de City Manager.

De aansturing van de City Managers verloopt via een ‘City Coach’. Dit is een ambtenaar in dienst van de gemeente die een cluster van City Managers begeleidt en controleert.

Om de City Manager in zijn taken te ondersteunen krijgt deze toegang tot diverse gemeentebronnen.

Allereerst krijgt de City Manager een officiële ID-kaart die zijn positie als City Manager bevestigt. Voor speciale gelegenheden (bijvoorbeeld tijdens publieke onrust) krijgt de City Manager ook een speciaal City Manager Jack waarmee zijn/haar aanwezigheid in de wijk duidelijk is voor iedereen.

De City Manager krijgt via een speciale Smartphone (de City Phone) toegang tot de informatie infrastructuur van Secure Haven. Via de City Phone kan de City Manager bijvoorbeeld extra informatie over buurtbewoners via diverse databases binnen en buiten de (gemeentelijke) overheid krijgen (inkomen, strafblad, lidmaatschappen). Met deze informatie kan de City Manager een betere inschatting maken van de buurtbewoners.

Maar naast het opvragen van informatie bij de gemeente kan de City Phone ook worden gebruikt om informatie uit de buurt naar de gemeente te zenden. Door middel van geavanceerde audio-, foto- en videofuncties kunnen wangedrag, vernieling en/of vervuiling worden vastgelegd en verstuurd naar de City Coach, welke zorg draagt voor de afhandeling. Dit beeld- en geluidmateriaal wordt door de gemeente gezien als onmisbaar in het bestrijden van overlast en kleine criminaliteit in de buurt. Door de City Phone wordt de City Manager als het ware de ogen en de oren van de gemeente in de buurt.

De City Manager heeft primair een voorbeeldfunctie voor de gemeenschap en wordt geacht om actief sociale controle uit te oefenen op medebewoners. Dit houdt in dat de City Manager buurtbewoners moet aanspreken op zaken als vernieling, vervuiling, overlast en ander wangedrag. In uitzonderlijke gevallen kan de City Manager in samenspraak met de City Coach, overgaan tot het maken van een officiële aantekening in het gemeentedossier van deze personen om de sociale controle in de wijk kracht bij te zetten. Om de City Manager te beschermen tijdens zijn werk zal deze via de City Phone gevolgd worden door de City Sentry, het onbemande vliegtuig (UAV) dat permanent boven de stad hangt.

De City Manager heeft niet alleen ‘corrigerende’ taken. Hij/zij krijgt ook financiële ondersteuning vanuit de gemeente om leuke en aansprekende integratie- en cohesie trajecten binnen de buurt te starten. Voorbeelden zijn kennismakingsborrels en straatfeesten.

Rapport Thema Technologie en Mensenrechten

Deel 2: vanuit de LRE-benadering



Gezicht op Den Haag vanaf de Delftse Vaart in de 17e eeuw

(Cornelis Springer, Kaspar Karsen, 1852)

Bron: <http://www.zwingelspaan.nl/kwartierstaat/kwstgenxiiia.html>

Deze illustratie, die sterke associaties oproept met een veilig, leefbaar en welvarend Den Haag, is gekozen om aan te geven dat we bij het schrijven van deze rapportage niet zijn vergeten dat een concept als 'Secure Haven' in den Haag (i) een historische context heeft, (ii) een maakbaarheidsaspiratie uitdrukt die natuurlijke grenzen kent en (iii) sterk verbonden is met de stand van de techniek.

Inhoudsopgave deel 2

1	INLEIDING.....	45
1.1	BESCHRIJVING THEMA	45
1.2	PROBLEEMSTELLING.....	46
1.3	VRAAGSTELLING	46
1.4	WERKWIJZE	46
1.5	INDELING	46
2	LRE VOOR SECURE HAVEN.....	47
2.1	INSTITUTIONELE ANALYSE VOOR SECURE HAVEN.....	47
2.2	VAN VISIE NAAR DOELSTELLINGEN.....	52
2.3	VAN DOELSTELLINGEN NAAR BELEID.....	53
3	BEOORDELING VAN AANBEVELINGEN	58
3.1	MATERIËLE MAAKBAARHEIDVEREISTEN EN LRE-RISICO'S	58
3.2	SOCIAAL	58
3.3	ECONOMISCH	59
3.4	INFRASTRUCTUREEL	60
3.5	INTERNATIONALE ORGANISATIES	61
3.6	VEILIGHEID.....	62
4	BEVINDINGEN EN VOORGESTELDE MAATREGELLEN	64
4.1	ANALYSE EN AANBEVELINGEN.....	64
4.2	MAATREGELLEN VOORGESTELD VANUIT LRE VOOR SECURE HAVEN	65
	BIJLAGE: KORTE THEORETISCHE VERANTWOORDING	67

1 Inleiding

Het rapport dat voor u ligt is een aanvullende uitwerking van de ideeën rondom het thema “technologie en mensenrechten”. Deze uitwerking borduurt voort op het inzicht dat de rechtswetenschap zich – bij een project als het Secure Haven project – niet kan beperken tot interpretatie en uitleg van bestaand recht. Het gaat bij een project als Secure Haven immers niet alleen om de (in het eerste deel van de rapportage over dit thema behandelde) vraag naar de juridische grenzen waarbinnen de voorgestelde oplossingen moeten blijven, maar ook om de kwaliteit van Secure Haven als een toekomstbestendig gereguleerd sociaal systeem.

Secure Haven is een institutionele aspiratie en een innovatieve dienst in voorbereiding. Als zodanig zijn er overeenkomsten met de uiteenlopende innovatieve diensten die op Internet ontstaan en die voorwerp zijn van rechtswetenschap. Geïnspireerd door werk uit verschillende disciplines wordt bij eLaw al enige tijd onderzoek gedaan naar bijdragen die de rechtswetenschap kan leveren waar het gaat om het ontwerpen van doeltreffende regelstelsels die de identiteit en de kwaliteit van gemeenschappen of instituties mede bepalen. In dit rapport wordt Secure Haven opgevat als zo’n institutie en wordt de bij eLaw ontwikkelde (en verder uit te bouwen) methode (die voorlopig “legal requirements engineering” is genoemd, of LRE) toegepast. Het doel is om te komen tot aanbevelingen in relatie tot nagenoemde opdrachten uit de beschrijving van werkpakket 1120:

- Mogelijkheden om pro-actief op te kunnen treden tegen (mogelijke) dreigingen, waaronder bijv. de mogelijkheden die door bestaande wetgeving worden geboden om méér gegevens te kunnen verzamelen indien gebruik gemaakt wordt van *privacy-enhancing technologies*.
- Conceptuele analyse van begrippen als ‘veiligheid’, waarmee de samenwerking tussen de verschillende disciplines gefaciliteerd kan worden, en aan de hand waarvan ook meer aanknopingspunten kunnen worden gegeven voor nog niet ingeschakelde disciplines, zoals deskundigheid op het gebied van ruimtelijke ordening.
- Het opstellen van een analysekader voor ‘grondrechtelijke toetsing’ van concepten/blauwdrukken zoals Secure Haven.

We zijn de opdrachtgevers erkentelijk voor de door hen geboden gelegenheid om een methode die nog slechts enkele malen in de praktijk werd gebruikt en derhalve nog nadere empirische toetsing behoeft bij dit project te kunnen inzetten en beproeven.

1.1 Beschrijving thema

Er zijn drie algemene doelen voor het Secure Haven project geformuleerd, te weten het produceren van een blauwdruk die voorziet in bestuurlijke maatregelen voor:

- adequate veiligheid binnen de internationale zone (IZ);
- een aantrekkelijk woon-, werk- en vestigingsklimaat binnen de IZ;
- economische groei voor de regio van vestiging door de uitstraling van de IZ.

Die algemene vragen worden behandeld vanuit verschillende disciplines en de behandeling is onderscheiden in meerdere thema’s. De centrale vragen van het voorliggende thema zijn:

- welke grondrechtelijke vragen worden opgeroepen door de infrastructuur die wordt voorgesteld in het project Secure Haven? (Deze vraag is in het eerste deel van de rapportage behandeld);
- *op welke wijze is de grondrechtelijke inkadering ingebed in meer algemene vragen over de relatie tussen mensenrechten en veiligheid?*

De beantwoording van deze laatste vraag is – met het oog op de ervoor genoemde algemene doelstellingen – voorwerp van het onderzoek waarvan in de voorliggende rapportage verslag wordt gedaan.

1.2 Probleemstelling

De vraag naar de wijze waarop de grondrechtelijke inkadering van de IZ als Secure Haven (veilig, aantrekkelijk vestigingsklimaat, economische aanjager voor de regio) is ingebed in *meer algemene vragen* over de relatie tussen mensenrechten en veiligheid is een Grote Vraag die uitnodigt tot een alternatieve rechtswetenschappelijke aanpak, in aanvulling op de meer gebruikelijke juridische analyse die in het eerste deel is uitgevoerd. Het onderzoek waar deze deelrapportage onderdeel van is heeft als doel om daarbij op te helderen welke kansen en risico's zijn verbonden aan het projectmatige, bestuurlijke streven naar de transformatie van de IZ van Den Haag tot een Secure Haven. In de kern is die vraag een *maakbaarheidvraagstuk*, anders gezegd: een *engineeringvraagstuk*, in het voorliggende geval gericht op de eigenschappen (veiligheid, leefklimaat, economische groei, algemene grondrechtelijke inkadering) van Secure Haven (een beoogd sociaal systeem).

1.3 Vraagstelling

Het project als geheel is gericht op het leveren van een blauwdruk voor Secure Haven. Daarmee is de opdracht voor deze rapportage om aan te geven op welke wijze de grondrechtelijke inkadering van Secure Haven *in die blauwdruk* is ingebed in meer algemene vragen over de relatie tussen mensenrechten en veiligheid. Die opdracht leidt tot het formuleren van drie vragen:

1. *Welk beoordelingskader leent zich voor de beoordeling van de maatregelen uit de blauwdruk?*
2. *Hoe moeten de maatregelen als voorgesteld in de blauwdruk voor Secure Haven worden beoordeeld vanuit het algemene beoordelingskader voor de relatie tussen mensenrechten en veiligheid?*
3. *Welke dreigingen en maatregelen voor het inrichten en verwezenlijken van Secure Haven vloeien voort uit dit algemene beoordelingskader?*

Dit zijn de drie vragen die in deze rapportage onder ogen worden gezien.

1.4 Werkwijze

Het onderzoek heeft, als onderdeel van het project, te maken met de bijzondere problematiek dat de het antwoord op de laatste twee vragen eigenlijk alleen kan worden gegeven nadat de resultaten van de andere deelprojecten gereed zijn. Vanuit die randvoorwaarde is de aandacht gedurende een belangrijk deel van het project gericht geweest op het beantwoorden van de eerste vraag en het (verder) ontwikkelen van de LRE-methodiek *in abstracto*. Gedurende de loop van het project heeft zich de gelegenheid voorgedaan om LRE nader toe te passen bij het beoordelen van functionele en technische specificaties bij enkele Europese aanbestedingsprojecten voor ICT-diensten en is daarbij van waarde gebleken. Omdat de verantwoording van de LRE-methodiek als rechtswetenschappelijke activiteit nogal theoretisch van aard is en nauwelijks van betekenis voor de toepassing ervan die hier centraal staat, is de wetenschappelijke verantwoording ervan ondergebracht in de Bijlage van dit rapport.

Één en ander houdt wel weer in, dat de beantwoording van de laatste twee vragen binnen de projectperiode noodzakelijkerwijze haastwerk is geworden, waarvan de sporen in deze rapportage zullen zijn terug te vinden. Daarvoor verontschuldigt de auteur zich bij voorbaat.

1.5 Indeling

In deze rapportage passen we eerst de LRE-methodiek toe op de maakbaarheidvraag voor Secure Haven (Hoofdstuk 2), waarna de aanbevelingen uit de andere deelprojecten worden beoordeeld en behandeld vanuit die methodiek (Hoofdstuk 3) en de conclusies en aanbevelingen (Hoofdstuk 4). In de Bijlage wordt de wetenschappelijke verantwoording voor de gehanteerde methodiek gegeven.

2 LRE voor Secure Haven

Het beoogde algemene juridische kader wordt hier getypeerd aan de hand van de volgende vraag:

Hoe organiseer ik mijn gedrag, als verantwoordelijke voor ontwerp en verwezenlijking van Secure Haven, als zorgvuldig en verantwoordelijk vanuit juridisch gezichtspunt - ook als de betreffende juridische kaders nog niet zijn uitgekristalliseerd?

De vraag haakt, in zijn algemeenheid, met name aan bij een centrale bepaling uit het Nederlandse civiele recht, als volgt neergelegd in artikel 6:162 van ons Burgerlijk wetboek (onrechtmatige daad):

1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.
2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.
3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

Artikel 6:162 Bw is een soort *catch-all* bepaling die aansprakelijkheid verbindt aan schade die is ontstaan door gedrag dat in strijd is met een wettelijke plicht *of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt*. Met name de laatste formulering is open en biedt ruimte aan meer algemene overwegingen van rechtvaardigheid en andere natuurrechtelijke noties. Aangenomen moet worden dat wat in het maatschappelijk verkeer betaamt gerelateerd is aan de mate van zorgvuldigheid die doorgaans wordt verbonden aan een maatschappelijke functie of rol. Voor rechtspositivisten is deze bepaling niet onverkort van toepassing op overheidshandelen; vanuit een natuurrechtelijk perspectief is het aannemelijk dat *elke* overheid in *elk* deugdelijk rechtssysteem aan de achterliggende strekking van deze bepaling, waaraan de verwoording in de wet weinig toe- of afdoet, onverkort gehouden is. Om deze reden is LRE ontwikkeld vanuit een natuurrechtelijk perspectief.

LRE is een methodiek voor het identificeren en specificeren van algemene juridische vereisten voor de inrichting en het realiseren van een dienst die vorm krijgt als een sociaal regelsysteem. Secure Haven wordt als zo'n dienst opgevat. In dit hoofdstuk wordt de methode toegepast om het algemene kader te schetsen voor de juridische beoordeling van de blauwdruk van Secure Haven. De presentatie is informeel. Voor meer rigoureuze definities en procedurebeschrijvingen zij verwezen naar de Bijlage.

2.1 Institutionele analyse voor Secure Haven

Het is allereerst van belang de beoogde institutionele structuur van Secure Haven in kaart te brengen om een indruk te krijgen van welke belangen spelen, wie belanghebbend zijn, wie mee en wie tegen zullen gaan werken, hoe de bevoegdheden zijn verdeeld en hoe de verantwoordingslijnen lopen, met welke culturen we te maken krijgen en dergelijke.

Over wat *instituties* zijn bestaan verschillende opvattingen in verschillende disciplines. Het is praktisch om de structuur van instituties verwant te zien aan de structuur van *spelen*, met hun eigen bevoegdheidsgebieden, doelen, regels, velden, spelers, officials, publiek, communicatielijnen, scheidsrechters, technische talen en, eventueel, bonden c.q. subculturen. Zodra we een verschijnsel in een dergelijke structuur kunnen beschrijven hebben we te maken met een institutie (of gereguleerd sociaal systeem).

Op basis van inventarisaties uit de andere deelrapporten geven we, zo goed en zo kwaad als dat gaat, een weergave van Secure Haven als institutie, geordend aan de hand van zeven vragen.

1. Hoe zit Secure Haven institutioneel in elkaar?

Het gaat om een beeld van Secure Haven, niet als gebied of project, maar als gerealiseerd, gereguleerd sociaal systeem.³¹ Om eraan te kunnen werken moet een aantal deelvragen worden beantwoord. Die vragen zijn direct gekoppeld aan invariant aanwezig geoordeelde elementen van instituties.³² Het zijn de volgende 12 deelvragen:

1.1 Welke belangen dient Secure Haven?

Veiligheid in en een aantrekkelijk leef- en vestigingsklimaat voor zijn (potentiële) deelnemers (waaronder internationale organisaties) in de IZ van Den Haag; het stimuleren van economische welvaart in de regio.

1.2 Aan welke externe regelgeving is Secure Haven onderworpen?

Die vraag valt voor het Nederlandse recht niet gemakkelijk te beantwoorden en is afhankelijk van verschillende dingen, bijvoorbeeld of Secure Haven als institutie een privaatrechtelijke, een publiekrechtelijke of een PPS status krijgt, dan wel een *sui generis* status als IO. In alle gevallen zullen kwesties van immuniteit, mandatering en delegatie moeten worden opgehelderd. Omdat de zorg voor veiligheid in Nederland vooral een overheidszorg is zal, bij een publiekrechtelijk georiënteerde oplossing vermoedelijk gezocht moeten worden naar wettelijke, dan wel verdragsrechtelijke legitimering.

Erg duidelijk is dit overigens niet. Onaannemelijk is bijvoorbeeld – om het meest extreme geval als gedachte-experiment te nemen, en los van de vraag naar de wenselijkheid ervan – dat Nederland zijn soevereiniteit over een gebied als Secure Haven *zou kunnen* prijsgeven, en afstaan aan de institutie Secure Haven, en het gebied daarmee bevrijden van daarvoor bestaande wettelijke en verdragsrechtelijke verplichtingen. Hiermee zij vastgesteld dat deze extreme variant *de facto* niet verder hoeft te worden behandeld. Hetgeen weer inhoudt dat Secure Haven als institutie hoe dan ook gebonden zal zijn aan de verdragsrechtelijke regels waaraan Nederland zich heeft gebonden.

Een bijkomende complicatie waarmee moet worden gerekend is dat belangrijke deelnemers aan Secure Haven, die uit de categorie Internationale Organisaties, zelf weer gebonden kunnen zijn aan niet-Nederlandse rechtsstelsels, aan bijzondere bilaterale verdragen waarin Nederland partij is en aan verdragen waaraan de IO wel en Nederland niet is gebonden. Een en ander kan tot anomalieën en dubbelzinnigheden leiden waar het gaat om regelstelsels waaraan (deelnemers aan) Secure Haven zijn gebonden. En kan de complexiteit van overleg ten behoeve van een heldere bevoegdheidsverdeling explosief verhogen.

1.3 Welke regelgeving- en handhaving- en conflictbeslechtingbevoegdheden heeft Secure Haven, en voor welk gebied?

Aannemelijk is dat de bevoegdheden – als ze al worden geëxpliciteerd en waar nodig overgedragen – beperkt worden tot interne regelgeving ten behoeve van de veiligheid en het vestigingsklimaat: we gaan er hier van uit dat het stimuleren van economische welvaart in de regio hiervan een epifenomeen kan zijn en alleen indirect vanuit Secure Haven via regelgeving zal kunnen worden gefaciliteerd.³³ Hier zijn verschillende mogelijkheden waaruit nog moet worden gekozen.

Bepalend zijn hierbij antwoorden op enerzijds de vraag of Secure Haven een privaatrechtelijke, een publiekrechtelijke of een PPS status krijgt, en anderzijds de vraag naar de geografische architectuur van

³¹ Deze rapportage wijkt af van de benadering in de overige rapportages ten behoeve van de blauwdruk: daar is ervoor gekozen om Secure Haven niet als een aparte institutie te denken, maar als een geïntegreerd deel van de gemeente Den Haag. Voor zover het gaat om een bepaalde regio waarin naar een bijzonder klimaat wordt gestreefd waartoe bijzondere maatregelen en diensten nodig zijn (inclusief bijbehorende bevoegdheden en verantwoordelijkheden) gaat het per definitie om institutionalisering – ook als die vorm zou krijgen in over verschillende bestaande diensten verspreide verantwoordelijkheden.

³² Zie voor een toelichting hierop de Bijlage.

³³ Zie ook: C.N. Teulings, A.L. Bovenberg and H. van Dale, *De cirkel van goede intenties: de economie van het publiek belang* (Amsterdam University Press, 2005).

Secure Haven (om de gedachten te bepalen noem ik twee uitersten: een omheind gebied c.q. een diffuus door de gemeente Den Haag verspreide verzameling van beveiligde percelen of delen van percelen).

1.4 Hoe zijn regelgeving, handhaving en conflictbeslechting met betrekking tot de specifieke jurisdictie binnen Secure Haven organisatorisch vormgegeven?

Ook hier moeten nog keuzen worden gemaakt en ook hier hangen de antwoorden af van het private, publieke dan wel PPS-karakter. Wel verdient het vanuit de rechtswetenschap de aandacht dat die organisatorische vormgeving – ook wanneer het om alternatieve rechtspleging gaat – kan zijn gediend met respect voor beginselen als verwoord in Montesquieu's triasleer en het EVRM.

1.5 Welke regels beschermen welke vrijheden van de deelnemers in Secure Haven?

Ook hier moeten nog keuzen worden gemaakt. Voor zover bij de deelnemers de bereidheid bestaat om voor de bijzondere beveiligingsfuncties van Secure Haven afstand te doen (in bijzondere gevallen en voor bijzondere doelen) van de grondrechtelijke bescherming van hun persoonlijke levenssfeer zij opgemerkt dat zulks, ten minste in beginsel, tot de praktische privaatrechtelijke mogelijkheden binnen de bestaande regelgeving behoort door daarover expliciete afspraken te maken (doelbinding en toestemming in het kader van de Wbp).

1.6 Wie zijn de deelnemers ('regelsubjecten') in Secure Haven?

- Deelnemende Internationale Organisaties.
- Deelnemende overige organisaties.
- Hun werknemers en hun gezinnen
- Hun gasten, bezoekers en leveranciers

1.7 Welke overtuigingen worden in Secure Haven gedeeld?

Een betrouwbare, hoogwaardige en efficiënte dienstverlening op de gebieden van beveiliging en vestigingsklimaat rechtvaardigen een zekere mate van investering in de vorm van gedeeltelijk afstand doen van rechten c.q. autonomie (bijvoorbeeld op het gebied van privacy of door onderschrijven van beleids- en gedragsregels).

1.8 Welke regels, beleidsregels en normen gelden binnen de jurisdictie van Secure Haven?

Ten aanzien van de veiligheid: dit kan nog niet precies worden uitgewerkt. Er zijn meerdere mogelijkheden die in het volgende hoofdstuk worden afgeleid uit en besproken aan de hand van maatregelen en scenario's die in de andere werkpakketten aan de orde zijn gesteld. Zeker is, dat wanneer het streven is naar een verhoogd niveau van veiligheid in Secure Haven ten opzichte van het beveiligingsniveau in de rest van de gemeente Den Haag er juridische vragen zijn (gelijkheid), net als wanneer beveiligingstalen voor de openbare ruimte worden overgedragen aan civielrechtelijke diensten (legitimiteit, rechtsbescherming).

Ten aanzien van het leef- en vestigingsklimaat: hier gelden, *mutatis mutandis*, dezelfde overwegingen als genoemd bij de vorige alinea.

Ten aanzien van de economische uitstraling: dit is een moeilijke kwestie waaraan in een apart thema aandacht wordt besteed. Vanuit juridische optiek dient te worden gewezen op de (met name in EU-verband) geldende mededingingsrechtelijke regels die voor de praktijk vooral vorm hebben gekregen in het aanbestedingsrecht. Om een voorbeeld te noemen: Secure Haven zou een hoogwaardige industrie binnen zijn gebied kunnen willen doen vestigen, omdat hoe dan ook aanmerkelijke investeringen moeten worden gedaan in innovatieve, hoogwaardige, technische apparatuur ten behoeve van maatregelen, te nemen vanuit het beveiligingsdoel. Het verwezenlijken van die wens zou wel eens door aanbestedingsregels kunnen worden bemoeilijkt.

1.9 Welke zijn de externe doelgroepen van Secure Haven?

- Hoogwaardige (internationale) organisaties die zich kunnen willen vestigen in Secure Haven en genoemde overtuiging delen.
- Bedrijven in de regio.
- De gemeente Den Haag, zijn bestuursdiensten, bedrijven en bewoners.
- Landelijke overheidsdiensten, waaronder met name te noemen de IND, de ministeries van BZK, Justitie, Financiën, Buitenlandse zaken en EZ.
- Landelijke politie- en veiligheidsdiensten als de KLPD, de AIVD, Douane, Verkeer & Waterstaat, Voedsel- en Warenautoriteit, etc.

1.10 Welke zijn de communicatiekanalen waarlangs informatie (ook over het functioneren van Secure Haven) intern en extern wordt uitgewisseld?

- Intern - ten behoeve van Secure Haven zelf: deugdelijke kanalen voor communicatie van het bestuur in de richting van de deelnemers en omgekeerd, met het oog (1) op de bekendmaking van regulering en beleid, (2) op de terugkoppeling door de deelnemers over de ervaren kwaliteit en gebreken daarvan en (3) op de evaluatie van de hechting door de deelnemers aan Secure Haven als institutie.
- Intern en extern - ten behoeve van de besluitvorming bij en handhaving van beveiliging: deugdelijke kanalen voor efficiënte communicatie tussen de uiteenlopende diensten/functionies onderling (opsporing, meldingen, sensor-output, brandweer, eerste hulp, OM).
- Intern en extern: ten behoeve van besluitvorming bij en handhaving van het leef- en vestigingsklimaat.

1.11 Aan welke instituties is Secure Haven hiërarchisch ondergeschikt (en voor welke bevoegdheden)?

- Afhankelijk van de juridische status – zie ook enkele eerdere overwegingen hierboven.

1.12 Uit welke instituties is Secure Haven verder intern organisatorisch vormgegeven?

Het antwoord is opnieuw afhankelijk van de juridische status die Secure Haven krijgt. Aannemelijk is hoe dan ook dat er deelinstituties wordt ingericht voor beveiliging, brandweer, eerste hulp (ook bij calamiteiten). Aannemelijk is voorts dat er instituties wordt ingericht ten behoeve van het leef- en vestigingsklimaat, die zelf zorgen voor of toegang bieden aan vanuit de doelstellingen adequate medische zorgvoorzieningen, onderwijsvoorzieningen, telecommunicatievoorzieningen, culturele voorzieningen, sportvoorzieningen, conferentievoorzieningen, bereikbaarheid, openbaar vervoervoorzieningen, parken, winkels, hotels, horeca en dergelijke.

Duidelijk is, dat op het moment van rapportage er nog onvoldoende bekend is om de institutionele analyse verder uit te werken. Dat betekent twee dingen.

Ten eerste: wanneer de weg naar de verwezenlijking van Secure Haven wordt vervolgd, dient deze analyse te worden herhaald en aangevuld naarmate meer informatie beschikbaar komt om bovengenoemde subvragen te beantwoorden.

Ten tweede: de LRE-methodiek berust op een uitgewerkte institutionele analyse van de dienst die centraal staat, bij voorkeur aangevuld met de institutionele uitwerking van gerelateerde instituties (waarmee communicatiekanalen bestaan) van tenminste één niveau – in beide richtingen: intern en extern. Omdat op dit moment nog geen beslissing is genomen over de juridische status van Secure Haven wordt hier verder, waar opportuun, volstaan met algemene overwegingen over de volgende vier schetsmatig aan te duiden mogelijkheden:

- Secure Haven is een bestuursdienst van de gemeente Den Haag (verder: SH-DH);

- Secure Haven is een op convenanten tussen Gemeente, Provincie, Rijk en Internationale Organisaties rustende (internationaal) publiekrechtelijke, ZBO-achtige *sui generis* organisatie (verder: SH-IZBO);
- Secure haven is een op convenanten en duurcontracten rustende organisatie voor publiek-private samenwerking (verder: SH-PPS);
- Secure Haven is een volledig naar 'de markt' gedelegeerde dienst in handen van een beursgenoteerde onderneming (verder: SH-BOND).

Afgezien van de grote verschillen in haalbaarheid van de benodigde overeenstemming tussen de constituerende partijen heeft elk van de genoemde varianten in juridische status zijn eigen publiekrechtelijke haken en ogen die met name gevolgen hebben voor de reikwijdte van de autonome bevoegdheden die Secure Haven als institutie zal kunnen verwerven.

In aansluiting op de institutionele beschrijving van Secure Haven zien we enkele vragen onder ogen die moeten worden beantwoord om een beeld te kunnen schetsen van de te verwachten mogelijk- en moeilijkheden.

2. Welke interne instituties passen niet in de functionele lijn?

Onder de functionele lijn wordt hier een hiërarchische organisatorische structuur verstaan. Vanuit LRE-gezichtspunt dienen die (deel)-instituties waarvan bestuurlijke onafhankelijkheid *functioneel* is bekend te zijn. Het gaat hier in elk geval om de 'parlementair controle-' en de 'rechtsprekende' functies, in overweging valt te nemen om de interne 'pers-' en 'onderzoekfuncties' buiten de functionele lijn te plaatsen. De vraag kan nog niet worden beantwoord omdat de blauwdruk tot dusver nog onvoldoende is uitgewerkt. Vanuit LRE-perspectief wordt volstaan met de kanttekening dat het inrichten van bedoelde onafhankelijk opererende deelinstituties aandacht en aanbeveling verdient.

3. Welke interne instituties onttrekken zich - of kunnen zich onttrekken - aan de functionele lijn?

Het gaat hier niet om de verzameling van autonome bevoegdheden van individuele deelnemers, de verzameling van 'vrijheden' die deelnemers benutten om hun kennis, kunde en creativiteit in te zetten om de hen opgedragen taken uit te voeren, de ruimte die hen in staat stelt zich te onderscheiden. *Die ruimte, die overigens van groot belang is voor de later te bespreken motivering van deelnemers en die we verder aanduiden als SH-RAID (de Ruimte voor Autonom Initiatief van de Deelnemers in Secure Haven), is immers geen institutie in de hier besproken zin.*

Waar het hier wel om gaat zijn deelinstituties die zich om uiteenlopende redenen aan de functionele lijn kunnen onttrekken. Een bekende reden is gebrek aan bevoegdheid, als aan te treffen bij adviesinstellingen. De belangrijkste reden om hier bij LRE aandacht te besteden is de mogelijkheid van sterke vormen van *kennisasymmetrie*, van situaties waarin een deelinstitutie zoveel meer expertise heeft over een bepaalde taak dan de hiërarchisch bovengeschatte instantie, dat toezicht eigenlijk niet meer mogelijk is of ernstig wordt bemoeilijkt. In Secure Haven kan zich deze situatie gemakkelijk ontwikkelen naarmate de beveiliging meer op technologische expertise gaat rusten. Er zijn ernstige theoretische³⁴ en praktische risico's aan verbonden (denk aan de ervaringen met videobewaking in Londen en met overheidsautomatisering in Nederland) die later aan de orde worden gesteld. Vanuit LRE-perspectief wordt hier volstaan met de kanttekening dat het ontstaan en voortbestaan van kennisasymmetrieën aandacht behoeft en dat maatregelen worden getroffen om ertegen te waken dat de (in elk geval theoretisch) ermee verbonden potentiële perversiteiten ook daadwerkelijk optreden.

4. Welke interne instituties kunnen via de functionele lijn normaal worden benaderd?

Deze vraag is een controlevraag: het dienen alle andere interne instituties te zijn dan die welke bij het beantwoorden van de vorige vraag naar voren kwamen.

5. Aan welke regels van welke instituties, die in de functionele lijn boven de RA staan, dient Se-

³⁴ Economen als Akerlof (George Akerlof, The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, 1970 pp. 488-500, Williamson (2005) en Myerson (2007) besteden er aandacht aan.

cure Haven zich te houden?

Het antwoord op deze vraag kan niet worden gegeven zolang de juridische status van Secure Haven onbekend is. Er valt wel iets over te zeggen: wanneer die juridische status van het type SH-DH is ligt het antwoord besloten in de reguliere staats- en bestuursrechtelijke gereguleerde bestuurspraktijk. Wanneer de vorm van het type SH-BOND is, ligt het antwoord besloten in de regulier civielrechtelijk, bestuursrechtelijk en strafrechtelijk gereguleerde private bedrijvigheid. Bij de twee andere typen (SH-IZBO en SH-PPS) gaat het om de convenanten en verdragen die er concreet vorm aan geven en is van alles mogelijk. In dit stadium kan vanuit LRE-gezichtspunt alleen worden opgemerkt dat duidelijkheid op dit gebied een noodzakelijke voorwaarde is voor een goed functionerende Secure Haven.

6. Welke interne en externe instituties hebben direct belang bij Secure Haven, en welke worden daardoor in hun traditionele positie en werkwijze bedreigd?

De antwoorden op de vraag welke interne en externe instituties belang hebben bij de beoogde dienst en welke in hun traditionele positie en werkwijze worden bedreigd zijn van belang om na te gaan waar extra aandacht zal moeten worden besteed aan het bewerkstelligen van adequate motivering binnen en adequate bereidheid tot samenwerking buiten Secure Haven omdat moet worden aangenomen dat anomalieën en dubbelzinnigheden bij de taakuitoefening en bevoegdheden van bestaande instituties veelal aanleiding vormen voor een vijandige houding.³⁵ Opnieuw is de inventarisatie afhankelijk van de juridische status, en daarmee van de organisatorische inrichting die Secure Haven zal krijgen. Aannemelijk is dat naarmate Secure Haven meer zelfstandige deelinstuties krijgt die zelfstandig verantwoordelijk worden voor taken die doorgaans elders zijn ondergebracht aan dit punt meer aandacht moet worden besteed. Gelet op de doelstellingen (veiligheid, leef- en werkklimaat en economische uitstraling) moet nadere aandacht voor genoemde anomalieën en dubbelzinnigheden onontbeerlijk en onvermijdelijk worden geacht. Veiligheidsdiensten, politie, brandweer, eerste hulp etc. komen in elk geval in aanmerking.

7. Hoe kunnen de instituties die door de inrichting van Secure Haven in hun autonomie worden bedreigd worden gemotiveerd om aan het project mee te werken en om de resultaten te aanvaarden?

Deze vraag kan pas worden gesteld en beantwoord nadat de vragen 1 t/m 6 meer volledig zijn beantwoord. Gevolg is, dat in deze rapportage de kwestie van motivering op een hoog niveau van abstractie blijft.

2.2 Van visie naar doelstellingen

Het institutionele model geeft een (zij het nog onvolledig) overzicht van de hele organisatorische inbedding van Secure Haven en van zijn afhankelijkheden. Nu de behandeling ervan is voltooid verscherpen we de focus op de beoogde dienst.

We rekenen daarbij terug, vanuit de doelstelling, aan de hand van de volgende vraag:

9. Wat is de visie die het streven naar Secure Haven ondersteunt?

De visie die het streven naar Secure Haven ondersteunt is in zekere zin een utopisch beeld, analoog aan het beeld als opgeroepen door de afbeelding op de titelpagina van dit rapport. De gemeente Den Haag huisvest een aanmerkelijk aantal internationale organisaties binnen haar grenzen en zoekt naar (en ziet) mogelijkheden om die situatie uit te bouwen naar een geïnstitutionaliseerde, gespecialiseerde dienst die zo aantrekkelijk is voor hoogwaardige internationaal georiënteerde organisaties, dat Secure Haven in Den Haag een (bijvoorbeeld Genève naar de kroon stekende) *hub* wordt voor de vestiging van die organisaties. Die visie is vertaald in drie doelstellingen:

- adequate veiligheid binnen de internationale zone (IZ);
- een aantrekkelijk woon-, werk- en vestigingsklimaat binnen de IZ;
- economische groei voor de regio van vestiging door de uitstraling van de IZ,

³⁵ Mede gebaseerd op Mary Douglas, *Purity and Danger*, Routledge & Kegan Paul, 1966.

en wel zodanig, dat Secure Haven tenminste even aantrekkelijk wordt als Genève, als vestigingsplaats voor hoogwaardige internationaal georiënteerde organisaties.

2.3 Van doelstellingen naar beleid

Ook op het algemeen niveau stuiten we opnieuw op moeilijkheden. Want wie gaat het beleid nu eigenlijk vormgeven en uitvoeren? Op dit moment wreekt zich opnieuw dat nog onduidelijk is welke de juridische status en bijbehorende bestuurlijk/organisatorische structuur van Secure Haven zal zijn, en welk type van geografische architectuur wordt gekozen. Om de analyse te kunnen voortzetten moet een keuze worden gemaakt, en dat zal ik hier ook doen, zij het met de kanttekening dat die keuze geen aanbeveling inhoudt – daarvoor heeft de opsteller van het rapport onvoldoende kennis over de belangen die spelen, over de verplichtingen die bestaan en over de politieke situatie – en als enige doel heeft om de methodiek verder te kunnen laten zien.

Dat neemt niet weg dat een keus moet worden gemaakt. Er zijn (als eerder aangeduid) vier mogelijkheden: SH-DH, SH-IZBO, SH-PPS en SH-BOND. Bij de verdere analyse wordt ervan uitgegaan dat SH-DH de juridische structuur wordt van Secure Haven.

Die keus zou als volgt kunnen worden verdedigd.

1. De problematiek van het optreden van anomalieën en ambiguïteiten tussen verantwoordelijke diensten wordt geminimaliseerd.
2. De inrichting van de verantwoordelijke organisatie heeft al goeddeels vorm gekregen en deze heeft ervaring met en bevoegdheden voor het treffen van maatregelen ten behoeve van de geformuleerde doelstellingen.
3. Het is niet alleen de IZ van den Haag die – in vergelijking met de andere gemeenten in Nederland – bijzondere zorg qua veiligheid vraagt: veel kwetsbare instellingen van staatsbelang zijn in Den Haag gevestigd (Parlementen, Regering, Ministeries, Hoge Raad, Raad van de Rechtspraak, Raad van State, Hofhouding, ambassades etc.), en lang niet allemaal in de IZ.
4. Vermeden wordt om onderscheid te maken tussen een wél- en een níet bijzonder beveiligd en anderszins bevoorrecht gebied binnen de gemeente Den Haag, hetgeen gemakkelijk zou kunnen worden opgevat als een door het bestuur ingerichte vorm van rechtsongelijkheid.
5. Voorkomen wordt dat (opnieuw) ingewikkelde (internationale) mandaterings-, delegatie- en samenwerkingsafspraken moeten worden gemaakt nog voordat Secure Haven in het leven kan worden geroepen (en dus: nog zonder de aantoonbare voordelen ervan te kunnen laten zien) zoals nodig zou zijn bij alle drie de andere juridische vormen.
6. Voorkomen wordt dat bevoegdheden die in Nederland traditioneel publiekrechtelijk van aard worden geacht (beveiliging, leef- en vestigingsklimaat) moeten worden opgedragen aan privaatrechtelijke organisaties, met de bijbehorende complicaties waar het gaat om toezicht en rechtsbescherming.
7. Intuïtief wegen deze zes voordelen ruimschoots op tegen het nadeel dat van de bewoners/deelnemers in SH-DH niet privaatrechtelijk kan worden overeengekomen, maar langs publiekrechtelijke weg moet worden gelegitimeerd. De bereidheid tot ‘meedoen’ (*compliance*) met de normen van SH-DH kan, bijvoorbeeld, niet via een afdwingbaar contractueel filter, voorafgaand aan vestiging worden geregeld. Iets wat bij SH-PPS en SH-BOND eerder tot de mogelijkheden zou behoren.

Nogmaals benadrukt zij dat deze keuze wordt gemaakt om de analyse te kunnen voortzetten, én omdat deze variant het beste aansluit op de benadering in de blauwdruk, waarin geheel van afzonderlijke institutionalisering wordt afgezien. Daarbij past de kanttekening dat die keus geen invloed heeft (of zou hebben gehad) op de gebruikte methodiek (die, desgewenst, zou kunnen worden toegepast op de alsdan nieuwe situatie).

De nu voorliggende vraag wordt:

10. Welke zijn de algemene kernvereisten van Secure Haven die de motivering van zijn deelnemers oproepen en in stand houden?

Het gaat hier (nog) niet om de motivering van specifieke groepen van deelnemers, waarvoor vermoedelijk toegespitste motiveringsvereisten gelden; het gaat om *algemene* vereisten.

2.3.1 *Wederkerigheid*

Het gaat allereerst om de waardering van de deelnemers voor wat ze aan waarde ontvangen door aan Secure Haven deel te nemen, in relatie tot hun bereidheid daarvoor iets terug te doen. Het hiermee samenhangende kernvereiste is *wederkerigheid*, dat wil (hier) zeggen: het vereiste dat deelnemen aan en aanbieden van Secure Haven als een *transactie* (of reeks van transacties) wordt gezien die voor beide partijen toegevoegde waarde heeft, nu nog los gedacht van wat die waarden *de facto* zijn. Dit vereiste, dat niet alleen ten grondslag ligt aan noties over economische efficiëntie is evenzeer van toepassing op de grondslag van wat wel de openbare orde en de ‘Rule of Law’ wordt genoemd. De achterliggende gedachte is dat wanneer er sprake is van wederkerigheid, die gedragskeuzen binnen het RAID-domein³⁶ rationeel zijn, die binnen de grenzen van de regels en de normen van de institutie blijven. Op die deelnemers die zich door deze rationaliteit (verder: SH-rationaliteit) laten leiden is nauwelijks toezicht nodig. En hoe groter het hun aantal, hoe sterker de institutie staat als gereguleerd sociaal systeem, als *community*, als gemeenschap.

De historie heeft geleerd dat wat hier de verhouding tussen het gereguleerde domein en het RAID-domein wordt genoemd³⁷ niet alleen een belangrijke rol speelt bij individuele wederkerigheidsbeoordelingen, maar een belangrijke focus is voor politieke tegenstellingen. Met andere woorden: het vaststellen, bekendmaken en onderbouwen van deze verhouding voor Secure Haven is een onmisbaar, buitenwetenschappelijk, politiek element bij de voorbereiding ervan.

2.3.2 *Waakzaamheid*

Aangenomen moet worden dat niet iedere deelnemer aan SH-DH zijn gedrag door bovenbedoelde SH-rationaliteit zal laten leiden. Hier is waakzaamheid geboden, omdat SH-irrationeel gedrag verschillende oorzaken kan hebben en verschillende uitwerking op de gemeenschap. Kortweg onderscheid ik vier categorieën van SH-irrationeel gedrag die een olopende bedreiging vormen voor de stabiliteit van de institutie: *onthechting*, *parasiteren*, *vandalisme* en *verzet*. *Onthechting* omdat het onverschillig staan tegenover de gemeenschap die bedreigt, wanneer hun aantal omvangrijk wordt. *Parasiteren*, omdat wanneer duidelijk wordt dat men weg kan komen met de voordelen zonder te investeren dat de motivering van de SH-rationele deelnemers aantast. *Vandalisme* omdat het moedwillig ‘voor de lol’ beschadigen van wat door de gemeenschap van belang wordt gevonden die gemeenschap ernstig kan beschadigen. *Verzet* omdat moedwillig, ‘uit overtuiging,’ beschadigen van de institutie een ander woord is voor terroristisch gedrag met onvoorspelbare schade als gevolg, dat tot uiteenvallen van de institutie leiden kan.

Het is een kernvereiste van Secure Haven, waar het om de motivering van zijn deelnemers gaat, om waakzaamheid ten aanzien van deze vormen van SH-irrationeel gedrag te mobiliseren en om zichzelf in een positie te brengen waar tenminste bekend is (1) wat de omvang is van de eerste twee categorieën en (2) wie wanneer tot de laatste twee categorieën van gedrag dreigen over te gaan.

2.3.3 *Weerbaarheid, proportionaliteit*

Aansluitend is voor de motivering van wie hier zich rationeel gedragende deelnemers worden genoemd dat Secure Haven in voorkomende gevallen laat zien tot effectieve maatregelen te kunnen overgaan. Waar het gaat om vandalisme en verzet zo nodig zelfs pro-actief. In direct verband met weerbaarheid en wederkerigheid staat daarbij de proportionaliteit van hierbedoeld optreden, het rekening houden met de maat der dingen, met het evenwicht tussen de inbreuk op belangen van deelnemers enerzijds en het gewicht van de daartoe aanleiding gevende redenen anderzijds.

³⁶ Zie hiervoor, onder vraag 1.12.

³⁷ Maar ook wel als de tegenstelling tussen (of het evenwicht tussen) regulering en vrijheid c.q. links en rechts, sociaal en liberaal etc. wordt aangeduid. Zie voor een opmerkelijke en omvangrijke strategisch-historische beschouwing mede hierover: Philip Bobbitt, *The Shield of Achilles: War, Peace and the Course of History*, Knopf, 2002.

2.3.4 *Betrouwbaarheid regulering en beleid*

11. Welke zijn de algemene kernvereisten van secure Haven, die het vertrouwen van zijn rationale deelnemers vestigen en in stand houden?

Voor het antwoord op deze vraag kies ik een benadering die diep verankerd ligt in het recht. Secure Haven wordt gerealiseerd in een gereguleerd sociaal systeem. En in de rechtswetenschap is al eeuwen belangstelling voor de vereisten waaraan geregleerde sociale systemen moeten voldoen om behoorlijk te zijn en vertrouwen te wekken. Aan de resultaten van die belangstelling ontleen ik de volgende negen algemene kernvereisten voor de betrouwbaarheid de regels van Secure Haven als beleid. Ik houd de toelichting beperkt omdat het om weinig controversiële, formele minimumvereisten gaat die zich in de discussies over de Rule of Law hebben gevestigd.³⁸ Ik noem ze verder Rule-of-Law vereisten.

Non-discriminatie

Regels moeten algemeen zijn en non-discriminatoire. Discriminatie is niet alleen ongrondwettelijk, het ontnemt perspectief aan en bederft de bereidheid tot participatie van wie worden gediscrimineerd.

Prospectief

Regels hebben geen terugwerkende kracht. Die figuur leidt tot willekeur, rechtsonzekerheid en wantrouwen en bederft daarmee de motivering voor deelname.

Helderheid en haalbaarheid

Regels moeten begrijpelijk en haalbaar zijn. Onbegrijpelijke regulering is *qualitate qua* onhaalbaar, onhaalbare regulering wordt beoordeeld als lege retoriek en lege retoriek leidt tot demotivering en onverschilligheid.

Stabiliteit

Regels zijn bedoeld om er gedrag mee in overeenstemming te brengen. Nieuwe regels vragen daarom extra inspanning van de deelnemers. Naarmate regels vaker worden aangepast neemt de last van die inspanning toe, en tast daarmee de wederkerigheidsevenwichten aan.

Integriteit

De bestuurlijke en beheerselites dienen zich aan hun eigen regels te houden op straffe van verlies aan vertrouwen. Hieraan kan een bijdrage worden geleverd door conflictbeslechting en toezicht op het bestuur in handen te leggen van een onafhankelijke deelinstituten.

Terugkoppeling

Het bestuur van Secure Haven kan vertrouwen winnen en behouden door publieke verantwoording en wanneer het openstaat voor terugkoppeling van deelnemers en daar ook iets mee doet.

2.3.5 *Kennis, kunde*

Een belangrijk en vanzelfsprekend aspect van betrouwbaar beleid heeft te maken met de op materiële deskundigheid rustende professionaliteit waarmee maatregelen en beleid door het bestuur van SH worden onderbouwd. Geklungel doet afbreuk aan vertrouwen en draagvlak. Dit is een belangrijk punt omdat een vermoeden bestaat dat de bestuurlijke verantwoordelijkheid, alleen en als zodanig, onvoldoende motiveert tot het steeds maar op hoog niveau ontwikkelen, bijhouden en inzetten van materiële kennis over de te reguleren situaties zoals blijkt uit te overvloedig inzetten van externe expertise. Er zijn kennelijk extra *incentives* nodig.

³⁸ Zie daarvoor bijvoorbeeld: Brian Z. Tamanaha, *On the Rule of Law*, Cambridge University Press, 2004.

Voorbeelden van wat hier mis kan gaan dringen zich overvloedig op bij de inzet van ICT-diensten door de Nederlandse overheden bij haar dienstverlening of beleidsuitoefening. Zie daarvoor een hele reeks van schokkende rapportages van de Rekenkamer (onder meer bij de Politie, P-direct, het UWV etc., etc.).

Net als bij, en verwant aan, de problemen die zich aandienen bij kennisasymmetrieën is deze kwestie van een zekere urgentie waar overwogen wordt om nieuwe technieken in te zetten ter ondersteuning van maatregelen ter beveiliging. Het onderwerp materiële kennis en kunde komt nader aan de orde in Hoofdstuk 3.

2.3.6 Algemene maakbaarheidvereisten voor Secure Haven

De voorafgaande opsomming van aspecten die in zijn algemeenheid van belang zijn voor beleidsuitoefening ten behoeve van een gereguleerd systeem als Secure Haven is daarmee tegelijkertijd een opsomming van functionele beleidsrisico's voor inrichting en voortbestaan ervan. Die risico's laten zich moeiteloos verbinden aan algemene vereisten waaraan voldaan moet worden (waarmee tenminste rekening mee moet worden gehouden) om Secure Haven te kunnen maken en in stand te houden. Het gaat, korthedshalve om de volgende risico's en vereisten:

Beleidsrisico	Algemeen maakbaarheidsvereiste
Wederkerigheid	Waardencalculus komt positief uit voor deelnemers
Waakzaamheid	Aantallen en plannen van 'SH-irrationelen' zijn bekend
Weerbaarheid	Pro-actief optreden bij ernstige dreigingen
Proportionaliteit	Maatregelen zijn in evenwicht met bedreigde belangen
Betrouwbaarheid	Rule-of-Law vereisten worden gerespecteerd
Materiële kennis en kunde	Toereikende materiële kennis en kunde zijn aanwezig

Tabel 1: Beleidsrisico's met maakbaarheidvereisten

Dat iets als maakbaarheidvereiste kan worden geïdentificeerd betekent nog geenszins dat het vereiste ook kan worden verwezenlijkt.

Onmiddellijk in het oog springt natuurlijk het eerste, aan *wederkerigheid* verbonden vereiste: de beoordeling van wat de deelname aan Secure Haven kost en wat die oplevert is aan de deelnemer, niet aan het bestuur. Vanuit de mensenrechten spelen hier overwegingen rond individuele vrijheden met de vrijheid van meningsuiting en, achterliggend maar niet direct reguleerbaar, de vrijheid van oordeelsvorming.

Ook voor bij het aan het beleidsaspect *waakzaamheid* gekoppelde maakbaarheidvereiste waar het gaat om informatie over (en kwalificatie van) de oordeelsvorming van de deelnemers en de rol die daarbij wordt gespeeld door wat eerder SH-rationaliteit werd genoemd zijn problemen te verwachten. Afgezien van de vraag of bedoelde informatie überhaupt in betrouwbare vorm zal kunnen worden verkregen speelt hier ook vanuit mensenrechtelijk gezichtspunt het vraagstuk van de bescherming van de persoonlijke levenssfeer.

Ten aanzien van het aan *weerbaarheid* gekoppelde vereiste van pro-actief optreden in die gevallen waarin beschikbare informatie daartoe aanleiding geeft zijn vermoedelijk minder problemen waar het gaat om de mensenrechten, tenminste wanneer binnen de wettelijke kaders wordt gebleven die de toepasselijke excepties van bedoelde rechten implementeren.

Waar het gaat om de drie laatstgenoemde maakbaarheidvereisten (verbonden aan *proportionaliteit*, *betrouwbaar*, *kennis en kunde*) zijn er geen argumenten die de feitelijke maakbaarheid in de weg staan, ook niet van-

uit mensenrechtelijke optiek – tenminste wanneer in aanmerking wordt genomen dat we hier de SH-DH variant bespreken.

2.3.7 *Algemene grenzen aan de maakbaarheid van Secure Haven*

Deze rapportage wordt, als gezegd, opgesteld vanuit een natuurrechtelijk gezichtspunt. Dat is van belang omdat daarmee argumentaties kunnen worden verbonden over de (grenzen aan) de werkzaamheid van hiërarchisch op gezag c.q. soevereiniteit rustende regulering. Aan deze argumentaties ligt een mechanistische kijk op de werking van gereguleerde sociale systemen ten grondslag. Ze worden hier opgevat als sociale, feitelijke fenomenen,³⁹ die aan bepaalde, empirisch kenbare wetmatigheden gehoorzamen. Waar het hier om gaat kan worden weergegeven in etiologische termen over functies.⁴⁰

Het gaat om een ogenschijnlijk circulaire functionele argumentatie. Waarom heeft de kamer een raam? Om voor licht en lucht te zorgen. Waarom is de kamer licht en vol frisse lucht? Omdat er een raam is. De functie van het raam *is* zijn bestaansgrond. Aangenomen wordt dat hetzelfde geldt voor Secure Haven. Waarom is Den Haag voorzien van een Secure Haven? Omdat het er veilig is, en goed toeven. Waarom is het veilig en goed toeven in Den Haag? Omdat het een Secure Haven is. Dit is de beoogde situatie.

Aan de maakbaarheidvraag voor Secure Haven kan dan worden verbonden dat we moeten weten hoe de gecombineerde functies van veiligheid en leefbaarheid kunnen worden *gemaakt*. De voorafgaande analyse heeft laten zien dat veiligheid niet kan worden gemaakt door het bestuur alleen, dat daarvoor de inzet van de deelnemers nodig is. De grenzen van de maakbaarheid van Secure Haven liggen daar, waar het bestuur de deelnemers niet toereikend kan motiveren tot SH-rationele gedragskeuzen.

2.3.8 *Materiële maakbaarheidvereisten*

Tot zover is vanuit een algemeen recht-systeem-theoretisch vertrekpunt dat werd toegepast op de notie van een Secure Haven, als gereguleerd sociaal systeem, in den Haag. De behandeling heeft een aantal, grotendeels voor zichzelf sprekende resultaten opgeleverd.

Nog niet is ingegaan op de vraag over de materiële inhoud van een en ander. Die wordt in het volgende Hoofdstuk aan de orde gesteld

³⁹ In de geest van de socioloog Durkheim, als verdedigd en uitgewerkt door Mary Douglas, *How Institutions Think*, Syracuse University Press, 1986.

⁴⁰ Naar Larry Wright, *Functions*, *The Philosophical Review*, April 1973, pp.139-168.

3 Beoordeling van aanbevelingen

Ter recapitulatie de drie vragen waarover deze rapportage gaat:

1. *Welk beoordelingskader leent zich voor de beoordeling van de maatregelen uit de blauwdruk?*
2. *Hoe moeten de maatregelen als voorgesteld in de blauwdruk voor Secure Haven worden beoordeeld vanuit het algemene beoordelingskader voor de relatie tussen mensenrechten en veiligheid?*
3. *Welke dreigingen en maatregelen voor het inrichten en verwezenlijken van Secure Haven vloeien voort uit dit algemene beoordelingskader?*

In het voorafgaande hoofdstuk is in Tabel 1 een antwoord gegeven op de eerste vraag. Het gaat om een kader dat voortvloeit uit een methodiek die is gebaseerd op een natuurrechtelijke benadering die antwoord kan geven op de vraag welke de sterktes, zwaktes en risico's zijn die kunnen worden verwacht bij inrichting en voortbestaan van een gereguleerd sociaal systeem. Dit kader wordt in het voorliggende Hoofdstuk toegepast om de materiële maatregelen die in de andere deelthema's van het project Secure Haven zijn voorgesteld te beoordelen. Daarmee wordt een antwoord gegeven op de tweede vraag. Daarna volgt in het vierde Hoofdstuk het antwoord op de derde vraag.

3.1 Materiële maakbaarheidvereisten en LRE-risico's

Ik heb thans de beschikking over een de volgende themarapportages:

1. Thema Sociale Omgeving
2. Thema Veiligheid
3. Thema Economie
4. Thema Functioneren van Internationale Organisaties
5. Thema Infrastructuur en Ruimtelijke ordening

Al die rapporten bevatten voorstellen voor maatregelen. In de navolgende paragrafen bespreek ik die voorgestelde maatregelen kort vanuit het algemene kader als weergegeven in Tabel 1. Ik volsta waar mogelijk met korte aanduidingen van de voorgestelde maatregelen. Die zijn immers in door de deelthema's zelf inhoudelijk besproken.

3.2 Sociaal

Op bladzij 19 van het rapport van het thema Sociale Omgeving zijn de volgende 11 maatregelen voorgesteld. Ze zijn letterlijk overgenomen (hier: genummerd voor referentie). Per aanbeveling geef ik overwegingen gebaseerd op het beoordelingskader als samengevat in Tabel 1:

1. Waar mogelijk sturen op een goede spreiding van autochtone, langdurig en kortstondig verblijvende expats in de buurt.
Onduidelijk is hoe deze maatregel weerstand biedt of kan bieden aan het op het eerste gezicht relevante wederkerigheidsrisico.
2. Het actief inzetten van langdurig verblijvende expats om de nieuw instromende expats wegwijs te maken in de buurt.
Onduidelijk is hoe deze maatregel past in de wederkerigheids calculus van de langdurog verblijvende expats.
3. Het oprichten van een Secure Haven Hospitality Desk waar nieuwe bewoners, bedrijven en ondernemers van de Secure Haven wegwijs worden gemaakt in alles wat met de Secure Haven en de buurt te maken heeft. Het genereren van het gevoel van welkom zijn.

Hieraan lijkt alleen het (goed vermijdbare) risico verbonden van ontoereikende kennis en kunde bij het personeel van de SHHD.

4. Het betrekken van alle belanghebbende partijen in de buurt voor het vormgeven van de fysieke en sociale omgeving van de buurt. Ontwikkel met de mensen en niet voor de mensen. De inbreng van de partijen moet terug te vinden zijn in het ontwerp of de maatregelen. Sociale cq. maatschappelijke betrokkenheid betekent vooral het samen zoeken naar oplossingen.
Hieraan lijkt alleen het (goed vermijdbare) betrouwbaarheidsrisico verbonden wanneer een onafhankelijke conflictbeslechtinginstantie zou ontbreken wanneer het met ‘mensen voor mensen’ proces daartoe aanleiding zou geven.
5. Betrokkenheid is blijvend. De vormgeving van een sociale omgeving is geen proces met een einde. Dit betekent ook dat na de ‘ontwerpfase’ de betrokkenheid een andere vorm kan krijgen, en in elk geval gevoed moet worden door heldere communicatie. Gedacht kan worden aan bijvoorbeeld een goed nieuws krant over Secure Haven.
Het betrouwbaarheidsrisico (goed vermijdbaar): bij terugkoppeling met of over alleen *goed* nieuws
6. Het is van belang te beseffen dat de verantwoordelijkheid ook met zich meebrengt, dat geen sprake kan zijn van (eindeloze of vrijblijvende) discussie, maar van dialoog om tot concrete besluiten en praktische oplossingen te komen zonder moeizame procedures. Deelnemen geschiedt op basis van vrijheid, maar niet op basis van vrijblijvendheid.
Zie de aantekening onder maatregel 4.
7. Creëer vanuit de Gemeente Den Haag binnen de Secure Haven de *Integratie Desk*. Deze desk is vraagbaak voor zowel de nieuwe Expats als de huidige bewoners van Secure Haven (al gevestigde expats en autochtone bewoners) die actief willen bijdragen aan het bevorderen van de sociale cohesie in Secure Haven en daarin gefaciliteerd willen worden. Hiermee wordt de drempel richting de overheid en andere van toepassing zijnde instanties laag gehouden. Deze desk kan ook fungeren als cultureel ontmoetingscentrum ter bevordering van de sociale cohesie in de Secure Haven buurt of straat.
Zie de aantekening onder maatregel 3. Misschien kunnen SHHD en ID worden geïntegreerd?
8. Omarm instituten die sociale cohesie in buurten of straten willen bevorderen
Het is niet helemaal duidelijk wat met omarmen wordt bedoeld.
9. Identificeer vanuit de gemeente sociaal bevlogen bewoners en Expats van de Secure Haven. Mensen die het vanuit intrinsieke motivatie belangrijk vinden om de sociale cohesie in de buurt te bevorderen. (Zie project ‘Buurtvaders en Buurtmoeders’ in Amsterdam). Ondersteun deze mensen waar nodig en koppel hen aan de Integratie Desk.
Past in de adressering van waakzaamheid- en weerbaarheidsrisico’s. Zorgvuldige omgang met de Wet bescherming persoonsgegevens lijkt aanbeveling te verdienen.
10. Betrek mensen met expertkennis op het gebied van integratievraagstukken ten behoeve van het proces.
Past in de adressering van kennis en kunde risico’s.
11. Stimuleer uitwisseling tussen internationale scholen en nationale scholen in Den Haag. Stimuleer gemengde scholen in de Secure Haven.
Zie de aantekening onder maatregel 1.

Niet alle voorgestelde maatregelen (met name 1 en 2) lijken zonder meer bij te dragen aan een positieve SH-rationele waardering.

3.3 Economisch

Op bladzij 22 t/m 27 van het rapport van het thema Economie zijn de volgende 4 maatregelen voorgesteld. De elementen ‘werking’ zijn overgenomen (hier: genummerd voor referentie). Per maatregel geef ik waar relevant overwegingen gebaseerd op het beoordelingskader als samengevat in Tabel 1:

1. Creëren van ideale vestigingsvoorwaarden.
2. Kennis en Laboratoriumstad R, V & V

3. Promoten stad van Vrede
4. Het kunnen aanbieden van (een) hoogwaardige congresfaciliteit (en) voor het houden van grote congressen

Geen van de aanbevolen maatregelen vormt, vanuit het LRE-kader gezien, een noemenswaardig risico. Misschien komen vragen van mededingingsrechtelijke aard op bij de verwezenlijking, maar daarvoor is nu nog onvoldoende bekend over de wijze waarop dat zal worden aangepakt.

3.4 Infrastructureel

Op de bladzijden 16 t/m 27 van het rapport over het thema Infrastructuur en Ruimtelijke Ordening zijn de volgende 23 maatregelen voorgesteld. Het element werkingsprincipe is hier weergegeven en de nummering van Hoofdstuk 2 van genoemd rapport is overgenomen. Per aanbevolen maatregel geef ik, waar opportuun, overwegingen vanuit het kader als samengevat in Tabel 1:

1. Het inzetten van verkeerscamera's voor security en assistentie van andere Dynamisch VerkeersManagement (DVM) maatregelen

Vermijdbaar betrouwbaarheidsrisico (integriteit) wanneer geen acht zou worden geslagen op de Wbp en de bijbehorende doelbinding.
2. Tracking van IO werknemers en/of familieleden middels RFIDs, GPS of GSM triangulatie.

Vermijdbaar betrouwbaarheidsrisico (integriteit) wanneer geen acht zou worden geslagen op de Wbp en de bijbehorende doelbinding.
3. Bij beperkte ruimte kan infrastructuur gebouwd worden om meerdere functies te herbergen, zoals ruimte voor wonen en werken, verkeer, groene ruimte, waterberging, recreatie, etc.
4. Door het optimaliseren van duurzame en/of natuurlijke zoneringen als een vijver, bomen, tuin en sculpturen wordt een stand-off zone gecreëerd dat de kwetsbaarheid van gebouwen tegen radicale acties vermindert en tijd vertragend werkt. Dit geldt met name voor ramkraken en zgn. *Vehicle Born Improvised Explosive Devices*.

Vermijdbaar wederkerigheidsrisico (waardencalculus) wanneer bedoelde belemmeringen de toegang van deelnemers en hun bezoekers onevenredig zou bemoeilijken.
5. Het ontwikkelen van een SH met een moderne, schone (wellicht zelfs futuristische) uitstraling, waarbij alle innovatieve vormgevingsaspecten worden gebruikt.
6. Door het sociale karakter van een wijk (of SH-zone) te versterken, wordt ook de toegankelijkheid voor bewoners (burgers, IO medewerkers) en recreanten vergroot.
7. Om de SH zone zelf veiliger te maken en te ontzien van zoveel mogelijk potentieel gevaarlijk verkeer (bezien vanuit zowel safety als security oogpunt) is het overstappen en gebruikmaken van alternatieve vervoerswijzen binnen en buiten de zone mogelijk.

Vermijdbaar wederkerigheidsrisico (waardencalculus) wanneer bedoelde alternatieve verkeersvormen extra belemmeringen blijken te zijn.
8. Een Virtual Secure Haven waarbij relevante informatie tussen IO's onderling en tussen IO's overheid en burgers kan worden gedeeld teneinde kennis beter te managen.
9. Een drijvend of opgespoten eiland voor de kust van Scheveningen.
10. Het certificaat Veilige Omgeving heeft betrekking op de inrichting van openbare ruimten, inclusief elementen als straatmeubilair en haltes voor het openbaar vervoer.
11. Door het stimuleren van alternatieve samenwerkingsvormen kunnen verbeteringen in het managen en de governance van veiligheid ontstaan.

3.5 Internationale organisaties

Op de bladzijden 16 t/m 27 van het rapport over het thema Internationale Organisaties zijn de volgende 11 maatregelen voorgesteld. Het element werkingsprincipe is hier weergegeven en de nummering van Hoofdstuk 5 van genoemd rapport is overgenomen. Per aanbevolen maatregel geef ik, waar opportuun, overwegingen vanuit het kader als samengevat in Tabel 1:

1. Voorlichten van alle NL-autoriteiten over immuniteiten van IO-werknemers.
2. Versoepelen verkrijgen van werkvergunningen.
3. Verbeteren toegankelijkheid voor IO's v/d Nederlandse arbeidsmarkt.
4. Het faciliteren van "uitwisselingsprogramma's" voor werknemers van IO's.
5. Versoepelen stagiarreregelingen.
6. Verbeteren aansluiting sociale voorzieningen.
7. Bieden van fiscale privileges voor alle IO-werknemers.
8. Instellen loketfunctie bij overheid met liaison officer.

Hieraan lijkt alleen het (goed vermijdbare) risico verbonden van ontoereikende kennis en kunde bij het personeel van de loketfunctie.

9. Veiligheids- en beschermingsloket.

Hieraan lijkt alleen het (goed vermijdbare) risico verbonden van ontoereikende kennis en kunde bij het personeel van de loketfunctie.

10. Faciliteren van samenwerking tussen IO's
11. Afspraken maken over (interne) beveiliging
12. Faciliteren informatiestromen
13. Beschermen tegen cyberaanvallen

Hieraan lijkt niet alleen het (goed vermijdbare) risico verbonden van ontoereikende kennis en kunde bij de dienst die de bescherming verzorgt; de technologische bevoegdheden die een dergelijke beschermingsfunctie met zich mee brengt is zelf weer een beveiligingsrisico vanuit het gezichtspunt van de gebruiker die de cyberinfrastructuur gebruikt voor het uitwisselen van vertrouwelijke informatie.

14. Stroomlijnen interfaces IO-gastland
15. Instellen van een Joint CommunicationTaskforce
16. Voorlichten van alle NL-autoriteiten over onschendbaarheid van IO-terreinen
17. Creëren gebiedsveiligheid ten behoeve van IO's
18. Instellen 'Internationale politie': politie specifiek voor IO-clusters
19. Aansluiten nieuwe IO's bij beveiligingsinfrastructuur door SH beveiligingsfonds.
20. Het gemeenschappelijk maken van detention units voor IO's
21. Opvang van IO-kwartiermakers
22. Faciliteren congresfunctie
23. Aanbieden verhuisservice m.b.t. publieke diensten en telecommunicatie

Het overgrote deel van de voorgestelde maatregelen lijkt substantieel te kunnen bijdragen aan de vermindering van het wederkerigheidsrisico, met name voor Internationale Organisaties.

3.6 Veiligheid

In het rapport over het thema Veiligheid is wel een opsomming van typen dreigingen opgenomen en een indeling van soorten maatregelen, maar concrete voorstellen worden niet gedaan, wel wordt een groot aantal mogelijkheden geopperd, verspreid door het document. Ik stel daaruit enkele mogelijke maatregelen samen en bespreek die hieronder.

Pro-actieve maatregelen

“Deze maatregelen zijn gericht op het wegnemen van structurele oorzaken van risico’s. Bijvoorbeeld het niet toestaan dat een bedrijf dat werkt met gevaarlijke stoffen zich vestigt of het verbieden van het vervoer van gevaarlijke stoffen langs een bepaalde route.”

Ik meen dat de voorgestelde waaier van maatregelen onder de noemer “weerbare infrastructuur” hier thuis hoort. Ik denk niet dat hier andere dan (vermoedelijk vermijdbare) wederkerigheidsrisico’s mee verbonden zijn wanneer de infrastructuur te veel belemmeringen opwerpt voor reguliere activiteiten.

Preventie(ve) maatregelen

“Dit zijn maatregelen die tot doel hebben het risico te beperken. Dit door het voorkomen dat een bedreiging via een kwetsbaarheid tot een verstoring leidt of door het beperken van de potentiële effecten die gemoeid zijn met een incident. Bijvoorbeeld verplichten van kleinere opslag- en transporttanks, plaatsen van een hek, aanbrengen van betere sloten, aanbrengen van redundantie of plaatsen van back-up systemen.”

Het komt mij voor dat deze categorie van maatregelen vooral geschikt is om bepaalde risico’s verbonden aan gebreken in kennis en kunde (ongelukken, ook rampzalige) buiten de deur te houden, maar ook om weerbaarheidsrisico’s tegemoet te treden, met name dat van vandalisme, zoals dat gekoppeld lijkt aan vieringen (Koninginnenacht, Nieuwjaar), betogingen en samenscholingen van voetbalfans.

Detectiemaatregelen

“hebben tot doel om in een zo vroeg mogelijk stadium een incident te detecteren en/of te signaleren, zodat zo snel als mogelijk actie (repressiemaatregelen) kan worden ondernomen; bijvoorbeeld plaatsen van rookmelders of camera’s.”

Hier gaat het, meen ik, met name om de waakzaamheidsrisico’s als aangeduid in en rond Tabel 1. De grote vraag is of we *kunnen* vaststellen (en zo ja hoe, en zo ja, op legitieme wijze, en zo ja, hoe betrouwbaar) van deelnemers en bezoekers aan Secure Haven of ze er een binding mee voelen, of ze erop willen parasiteren, of ze vandalisme in de zin hebben dan wel er om ideële c.q. rancuneuze redenen schade aan willen berokkenen. Technische mogelijkheden die de detectie binnen bereik zou kunnen brengen zijn er legio – en als ze er nog niet zijn komen ze zeer binnenkort beschikbaar.⁴¹ Gigantische verzamelingen persoonsgebonden gegevens (uiteenlopend van telecommunicatieverkeergegevens via Google *logs* tot boodschappenprofielen bij Albert Heijn – naar willekeur aan te vullen met GBA en Wia-gegevens, gegevensverzamelingen van (sensen/camera’s van) gemeentes, politie, justitie, de IND en de AIVD) zouden kunnen worden ingezet om hieraan te werken.

Deze mogelijkheid stelt ons voor een van de grote politieke en maatschappelijke dilemma’s van onze tijd: we hebben de mensenrechten ingericht ter bescherming van de individuele burger tegen machtsmisbruik door de overheid, en we zijn nu, mede door de democratisering van de techniek, in het stadium dat de aandacht uitgaat naar het beschermen van de overheid tegen individueel (terroristisch) machtsmisbruik met onvoorspelbaar omvangrijke schade. De situatie heeft al op meerdere fronten geleid tot het wettelijk toestaan van uitzonderingen op de mensenrechten, met name de privacy – een trend die nog niet aan zijn einde is gekomen, zo lijkt het.

⁴¹ Informatici verzekeren ons dat “ubiquitous computing” voor de deur staat – waarmee ze bedoelen dat ons dagelijks leven doordringt wordt van digitale dienstverlening die wordt verzorgd door de combinatie van korrelkleine computertjes en sensoren. De RFID-chip in OV-kaarten is een voorbode.

Wanneer ik er, bij wijze van gedachte-experiment, van uitga dat alle genoemde informatie voor beveiligingsdoeleinden van Secure Haven beschikbaar zou komen, dan worden de risico's verbonden aan gebreken in waakzaamheid en weerbaarheid vermoedelijk aanmerkelijk verminderd, maar nemen de alsdan extra van belang te oordelen risico's van gebreken in proportionaliteit, in betrouwbaarheid en in kennis en kunde even zo sterk toe. Zolang daarvoor geen nadere oplossingen zijn gevonden die in wet en regelgeving zijn uitgekristalliseerd verdient het aanbeveling dat Secure Haven zodanig wordt ingericht, dat met die risico's rekening wordt gehouden.

Een voorbeeld om de gedachten verder te bepalen. Kort geleden, op 12 maart 2009, werden zeven personen op basis van een anoniem telefoontje verdacht van het voorbereiden van een terroristische aanslag en in hechtenis genomen. Voorts werd een winkelgebied gesloten voor het publiek. Na verloop van tijd werd de verdenking minder aannemelijk en zeker minder acuut, zodat niet alleen de verdachten weer in vrijheid werden gesteld, maar ook ernstig rekening moet worden gehouden met de omstandigheid dat ze ten onrechte werden verdacht. Waar het me om gaat is vast te stellen dat bij een verhoogd risico een verhoogde (ook proactieve) beveiliging past, en dat daarmee weer een verhoogd risico hoort op het treffen van maatregelen, waarvan achteraf blijkt dat ze onnodig waren. Dergelijk onnodig optreden kan misschien niet steeds worden voorkomen, maar wel kan er mee worden gerekend dat de daarmee aan te richten schade de wederkerigheid zal aantasten wanneer geen maatregelen worden getroffen en bekend gemaakt hoe de aangerichte schade (met name de reputatieschade) wordt weggenomen of wordt hersteld.

4 Bevindingen en voorgestelde maatregelen

De overwegingen uit de vorige Hoofdstukken leiden tot een aantal bevindingen die aansluiten op de opdrachten en gerelateerde vragen van werkpakket 1120, en tot vier maatregelen die vanuit LRE-optiek worden voorgesteld bij de verdere inrichting van Secure Haven.

4.1 Analyse en aanbevelingen

Hieronder zijn de vragen zoals die in de inleiding werden beschreven en voorzien van bevindingen die analytisch voortvloeien uit de gehanteerde methode:

- Mogelijkheden om pro-actief op te kunnen treden tegen (mogelijke) dreigingen, waaronder bijv. de mogelijkheden die door bestaande wetgeving worden geboden om méér gegevens te kunnen verzamelen indien gebruik gemaakt wordt van *privacy-enhancing technologies*.

De positiefrechtelijke analyse van deze vraag is gegeven in het eerste deel van de rapportage over werkpakket 1120. Vanuit LRE-optiek kan erop worden gewezen dat het *gebruik van privacy-enhancing technologies* (als technieken die de band tussen gegevens en de betreffende persoon doorsnijden) vermoedelijk weinig te bieden heeft waar het gaat om rechtsbescherming tegen de voor pro-actief optreden benodigde verzameling en bewerking van tot personen te herleiden informatie: dat is nu eenmaal het (legitieme) doel van het aanleggen en bewerken van die verzamelingen. De benodigde bescherming dient misbruik en verkeerd gebruik te beteugelen, en *daarvoor zijn privacy enhancing technologies* naar hun aard niet geschikt.

- Conceptuele analyse van begrippen als ‘veiligheid’, waarmee de samenwerking tussen de verschillende disciplines gefaciliteerd kan worden, en aan de hand waarvan ook meer aanknopingspunten kunnen worden gegeven voor nog niet ingeschakelde disciplines, zoals deskundigheid op het gebied van ruimtelijke ordening.

Vanuit LRE-optiek is het begrip veiligheid te relateren aan vijf verschillende houdingen die bij personen binnen en buiten het betreffende sociale systeem (*in casu* Secure Haven) kunnen postvatten: SH-rationeel, onthecht, parasiterend, vandalisme-bereid, bereid tot verzet. Over hoe die houdingen effectief kunnen worden gediagnosticeerd op basis van beschikbare gegevens is weinig bekend – onzeker is of die kennis überhaupt kan worden verworven. Bedoelde kennis ligt in eerste instantie in de belangstellingssfeer van de sociale wetenschappen, met name de sociale psychologie, de sociologie, de anthropologie en de criminologie maar speelt ook een rol in de economie, de rechtswetenschap, de politieke wetenschap en de informatica.

- Het opstellen van een analysekader voor ‘grondrechtelijke toetsing’ van concepten/blauwdrukken zoals Secure Haven.

LRE biedt geen analysekader voor de grondrechtelijke toetsing van concepten als Secure Haven – daarvoor past de positiefrechtelijke benadering als gegeven in het eerste deel van de rapportage in werkpakket 1120. LRE biedt wel een aanvullend analysekader voor het toetsen van de wijze waarop rekening is gehouden met de natuurlijke waarden welke geacht worden zin te geven aan grondwettelijke toetsing.

- Welk beoordelingskader leent zich voor de beoordeling van de maatregelen uit de blauwdruk?

Voor het beoordelen van de maatregelen uit de blauwdruk zijn meerdere kaders relevant, waaronder dat van het positieve recht en dat van het democratische proces. LRE leent zich als aanvullend kader voor het beoordelen van voorgestelde maatregelen, als weergegeven in het vorige hoofdstuk.

- Hoe moeten de maatregelen als voorgesteld in de blauwdruk voor Secure Haven worden beoordeeld vanuit het algemene beoordelingskader voor de relatie tussen mensenrechten en veiligheid?

Zie, vanuit het LRE-kader, het vorige hoofdstuk.

- Welke dreigingen en maatregelen voor het inrichten en verwezenlijken van Secure Haven vloeien voort uit dit algemene beoordelingskader?

Zie, vanuit het LRE-kader, de volgende paragraaf.

4.2 Maatregelen voorgesteld vanuit LRE voor Secure Haven

Maatregel LRE-01	Rekening houden met wederkerigheid
Werkingsprincipe	Motiveren c.q. demotiveren van deelname aan Secure Haven
Beschrijving	Waardencalculus door deelnemers waarbij de voordelen van deelname worden afgewogen tegen de voor deelname benodigde investeringen
Noodzaak	Inrichten en in stand houden van Secure Haven als gereguleerd sociaal systeem
Relaties met (sub)thema's	Alle

Maatregel LRE-02	Beveiligingsinformatie vergaren, bewerken en interpreteren
Werkingsprincipe	Zo goed mogelijk onderscheiden van deelnemers, parasieten vanden en terroristen
Beschrijving	Vergaren en bewerken van gegevensverzamelingen
Voorwaarden	Nationale en internationale samenwerking met en signalering tussen opsporings- en veiligheidsdiensten
Noodzaak	Neemt toe naarmate de omvang van de schade die door individuen kan worden aangericht toeneemt en de bereidheid tot vandalisme en terrorisme bestaat
Voordelen	Bijdragen aan veiligheid
Nadelen	Mogelijkheden tot misbruik van informatie door overheidsdiensten neemt toe
Relaties met (sub)thema's	Mensenrechten, veiligheid

Maatregel LRE-03	Maak beleid voor pro-actief optreden bij ernstige dreigingen
Werkingsprincipe	Bijtijds verstoren, voorkomen; actie soms op basis van onzekere informatie of onzekere interpretatie van informatie
Beschrijving	Beoordelen van en optreden naar aanleiding van beschikbare beveiligingsinformatie die een specifieke dreiging indiceert
Voorwaarden	Integriteit, kennis en kunde bij de handhavers; bekendheid en acceptatie in de gemeenschap van de risico's behorende bij achteraf gebleken onnodig optreden
Noodzaak	Neemt toe naarmate de omvang van de schade die door individuen kan worden aangericht toeneemt en de bereidheid tot vandalisme en terrorisme bestaat
Voordelen	Veiligheid
Nadelen	Risico van en schade bij onnodig optreden; risico van misbruik van informatie
Relaties met (sub)thema's	Mensenrechten, veiligheid

Maatregel LRE-04	Zorg voor adequate kennis en kunde bij de gemeente en de betreffende diensten
Werkingsprincipe	Kennisasymmetrieën brengen risico's met zich mee waar het gaat om vertrouwen, en de mogelijkheid van misbruik van vertrouwen. In situaties waarin kennisasymmetrie een rol speelt kan één van de bij een transactie betrokken partijen de voorstellen en de waarachtigheid van de ander niet goed beoordelen.
Beschrijving	De situatie doet zich voor bij transacties tussen verschillende disciplines (bijvoorbeeld: bestuurders en ICTers)
Voorwaarden	Het borgen van de benodigde expertise bij de afhankelijke diensten
Noodzaak	Een betrouwbare 'verdeling van arbeid' over de verschillende spelers in een secure haven

Voordelen	Invloed op de betrouwbaarheid van de 'verdeling van arbeid'
Nadelen	Kosten
Relaties met (sub)thema's	Alle

Bijlage: korte theoretische verantwoording

Op welke wijze is de grondrechtelijke inkadering ingebed in meer algemene vragen over de relatie tussen mensenrechten en veiligheid?

In deze korte theoretische verantwoording wordt veelvuldig gebruik gemaakt van verwijzingen naar de literatuur, weergegeven in de Bibliografie. Het gaat in veel gevallen om bijdragen die de kiem hebben gelegd voor hele 'scholen' van onderzoek en wetenschappelijke discussie.

4.2.1 Een vermoeden als vertrekpunt

Er is een zekere verwantschap tussen de informaticadiscipline en de rechtswetenschap: beide houden zich bezig met regels en hoe ze werken.

Er is ook een verwantschap tussen de toepassing van beide disciplines: beide reguleren door middel van regels (Lessig 1999).

En er is nog een verwantschap: het succes van juridische- en van informaticaregelstelsels binnen hun werkingssfeer is afhankelijk van de mate waarin hun 'subjecten' bereid en in staat zijn zich aan de regels conformeren (Schreiber 2000, Radbruch 1948, Fuller 1967, Greif 2006) en aan de mate waarin zij hun deelnemerschap als 'toegevoegde waarde' ervaren.

Voorts is er een verwantschap tussen juridische en informaticaregelstelsels in de zin dat het om maakwerk gaat. Inrichting en onderhoud van computerprogramma's én van recht-stelsels is een kwestie van ontwerp (Schmidt 1986).

Tenslotte is er een geheel andere, belangrijke relatie tussen computerprogramma's en recht-stelsels groeiende: steeds meer functies van recht-stelsels zijn afhankelijk van of worden overgelaten aan ICT-diensten. Daaraan zijn risico's verbonden (Lessig 2000, Schmidt 2003, 2007).

Beoordeling van de kwaliteit van recht-stelsels is moeilijk (Radbruch 1946). Beoordeling van gebreken in computerprogramma's is eenvoudiger. In de jaren 1970-2000 is in de informatica veel wetenschappelijke aandacht besteed aan methoden voor het ontwerpen van deugdelijke ICT-diensten. De uitkomsten van dat onderzoek hebben geleid tot vergaande convergentie (bijvoorbeeld: Wieringa 1997, Scheiber et. al. 2000).

Misschien valt er iets – via analogische analyse - van die methoden te leren voor de rechtswetenschappelijke beoordeling van de inrichting van recht-stelsels. Dit vermoeden is in potentie relevant bij de beoordeling van hoe de grondrechtelijke inkadering van het ontwerp van Secure Haven is ingebed in meer algemene vragen over de relatie tussen mensenrechten en veiligheid. LRE is er het resultaat van.

LRE is ontstaan uit noodzaak. De rechtswetenschap houdt zich vrijwel uitsluitend bezig met de interpretatie van het positieve recht – dat wil zeggen: het beoordelen van situaties die plaats hebben gevonden (of denkbaar plaats zouden kunnen vinden in de toekomst) in het licht van het geldende recht op het moment van beoordeling. Die benadering is niet voldoende wanneer het om maatschappelijke innovatie gaat. Alsdan speelt tevens de vraag hoe het positieve recht zou moeten veranderen om die innovatie op een kwalitatief niveau te kunnen accommoderen. Die vraag vereist een methode waarin duidelijk is wat wordt verstaan onder de kwaliteit van het positieve recht en over ontwerpvereisten die ertoe leiden dat aanpassingen van het positieve recht een systeem bewerkstellingen dat van voldoende kwaliteit zal zijn om de innovatie onder ogen te zien.

Secure Haven is – als verwezenlijkt – een product van maatschappelijke innovaties: het omvat diensten die een nieuw niveau van veiligheid beogen te brengen waarbij onder meer gebruik wordt gemaakt van de nieuwe mogelijkheden die de informatica te bieden (zullen) hebben. Als zodanig is een LRE-analyse van de blauwdruk van Secure Haven gewenst.



Er zijn natuurlijk bezwaren aan te voeren tegen de vergelijking van ICT-diensten met recht-systemen, en, daarmee, tegen het vermoeden van geldigheid van methodische ‘transplantaties.’ In het vervolg van deze verantwoording bespreek (en verwerp) ik kort enkele van die bezwaren.

4.2.2 *Instituties*

Het eerste bezwaar betreft de verwantschap die hier wordt aangenomen te bestaan tussen ICT-diensten en recht-systemen.

Bij een analogische benadering wordt gezocht naar verwantschap op een hoger niveau van abstractie, naar verwantschap in structuur. Mijn stelling is dat zowel ICT-diensten als recht-systemen de structurele kenmerken vertonen van instituties.

Over wat instituties zijn bestaan verschillende opvattingen in verschillende disciplines. Misschien is het in praktische zin het meest voor de hand liggend om de *structuur* van instituties verwant te zien aan de structuur van subculturen, of, misschien beter nog, van spelen, met hun eigen doelen, regels, velden, spelers, officials, communicatielijnen, scheidsrechters, technische talen en, eventueel, bonden c.q. subculturen. Instituties hebben ook generieke *functies*: het genereren van regelmatigheden in sociaal gedrag en het creëren van helderheid over en draagvlak voor welk gedrag gevaarlijk is voor het voortbestaan van de institutie (‘openbare orde’ excepties). En instituties zijn *duurzaam* (kunnen dat zijn, streven er vaak naar): ze hebben de eigenschap dat ze kunnen voortbestaan, dat hun levensduur onafhankelijk is van de levensduur van hun ‘leden.’ Tenslotte: instituties hebben *identiteit*, het zijn ‘sociale feiten.’

Zodra we een verschijnsel in een dergelijke structuur functioneel kunnen beschrijven hebben we te maken met een institutie. Elders⁴² heb ik er het volgende over gezegd:

‘Institution’ is a family concept; it is hard to define, because institutions differ in many significant ways. Nevertheless I contend that it makes sense to consider anything showing the thirteen mentioned characteristics to be an institution. Thus, I consider *e.g.* the following kaleidoscopic collection of social systems to be institutions: the Dutch health care system, nation states, soccer world championships, families, parishes, pop groups, the UN, the EU, Mogadishu factions, firms, Super Bowls, schools, the Camorra, markets, games and most Internet-mediated services (Google, open source projects, Freenet, Wikipedia, Hyves, YouTube, Second Life, etc.), even Internet itself (with its IETF).

From a law-science perspective, the most striking characteristic of an institution is its having rules.⁴³ That is why I sometimes tend to call institutions ‘legal systems’ (when referring to nation states or treaty organizations) or ‘law systems’ (as synonymous to institutions in general).

Instituties oefenen een grote aantrekkingskracht uit op verschillende wetenschappen. Politieke filosofie (Montesquieu 1758, Smith 1776), institutionele economie/sociologie (Tilman 2002, refererend aan Durkheim en Veblen rond 1900), nieuwe institutionele economie (Coase 1937, Williamson 2005), economische geschiedenis (North 1991, Greif 2006), institutionele sociologie (Durkheim 1910), institutionele antropologie (Douglas 1971), institutionele rechtswetenschap (Montesquieu 1758, Hart 1961, Fuller 1963) vormen alle respectabele en duurzame (zij het thans niet altijd even modieuze) deeldisciplines.

Met name in de rechtswetenschap bestaat discussie over de vraag of deze zich bezig zou moeten houden met andere instituties dan die van soevereine jurisdicties, met ander recht-systemen dan statelijke rechtssystemen. Ik volg hier de opvatting van Fuller (1963: 154), die binnen de rechtswetenschap overigens thans niet erg

⁴² Aernout Schmidt, Radbruch in Cyberspace: about law-system quality and ICT innovation, thans bij de uitgever.

⁴³ Also, from an economic perspective, see North, D. 1990, ‘Institutions, Institutional Change and Economic Performance,’ Cambridge University Press.

dominant is. (Ik gebruik de term ‘recht-systeem’ voor instituties, gezien vanuit rechtswetenschappelijk perspectief, in plaats van de term ‘rechtssysteem’ voor statelijke jurisdicties en hun rechtsregels. Rechtssystemen zijn species van het genus recht-systeem).

In de Tabel 1 geef ik de structuur van instituties zoals ik hem zie.

<i>Institutie</i>	
<i>Identiteit</i>	<i>Naam</i>
<i>Belangen</i>	<i>Verzameling belang-waarde combinaties</i>
<i>Jurisdictie</i>	<i>Verzameling doel-gebied combinaties</i>
<i>Vrijheden</i>	<i>Verzameling doel-openbare orde beperkingen combinaties</i>
<i>Regels</i>	<i>Verzameling geldt als-leidt tot combinaties</i>
<i>Beleid</i>	<i>Verzameling geldt als-leidt tot combinaties</i>
<i>Normen</i>	<i>Verzameling geldt als-leidt tot combinaties</i>
<i>Elites</i>	<i>Verzameling geldt als-leidt tot combinaties</i>
<i>Werkers</i>	<i>Verzameling interne instituties</i>
<i>Doelgroepen</i>	<i>Verzameling actoren (individuen)</i>
<i>Overtuigingen</i>	<i>Verzameling (interne en externe) instituties</i>
<i>Feedback kanalen</i>	<i>Verzameling geldt als-leidt tot combinaties</i>
<i>Heeft instituties</i>	<i>Verzameling interfaces en protocollen tussen instituties</i>
<p><i>Functies van (regels van) instituties – het genereren van:</i></p> <p><i>(i) regelmatigheden in sociaal gedrag</i></p> <p><i>(ii) gemeenschappelijk gedragen ‘openbare orde’ beperkingen</i></p>	

Tabel 1: De structurele elementen van instituties

Als gezegd, het is mijn stelling dat zowel statelijke jurisdicties als succesvolle ICT-diensten (bijvoorbeeld: de sociale systemen waarin Google, of de Gemeentelijke Basisadministratie een centrale rol spelen) instituties zijn in bovenbedoelde zin. En dat het zin heeft om bij de beoordeling van voornemens om nieuwe sociale systemen in te richten de betekenis van de betreffende institutionele structuren te analyseren. Het is dan ook geen wonder dat de institutionele analyse een belangrijk onderdeel is van zowel eerdergenoemde ICT-methoden als van LRE.

Secure Haven is in bovengenoemde zin een institutie die vanuit LRE perspectief kan worden onderzocht. Het is, bijvoorbeeld, van belang de beoogde institutionele structuren (zowel hiërarchisch als lateraal) van de beoogde organisatie in kaart te brengen. Al was het alleen maar om een indruk te krijgen van welke belangen spelen, wie belanghebbend zijn, wie mee en wie tegen zullen gaan werken, hoe de bevoegdheden en de verantwoordingslijnen lopen en met welke culturen Secure Haven te maken krijgt.

4.2.3 Succesvolle instituties

Instituties zijn maakbaar. Maar zijn *succesvolle* instituties dat ook? Deze vraag behoort tot de moeilijkste en hardnekkigste uit de sociale wetenschappen en ik ga hem hier niet beantwoorden. Wat ik wel doe is een werkhypothese ontleen aan de twee meest succesvolle theorieën over de kwaliteit en ontwikkeling van (sociale en biologische) systemen die we kennen:

1. de werking van de ‘onzichtbare hand’ die door Smith (1776) is verbonden met het prijsmechanisme van de markt en de welvaart van staten (*marktwerking*),

en

2. de werking van het mechanisme dat door Darwin (1859) wordt verbonden aan de combinatie van (i) random mutaties in generaties van biologische organismen en (ii) de geschiktheid van het resultaat om te overleven onder de condities die de leefomgeving stelt (*natuurlijke selectie*).

De verwantschap tussen beide theorieën is in brede kring (h)erkend, al is er discussie over de vraag of Darwin, die in essentie over individuen en soorten gaat ook toepasselijk zou kunnen zijn op sociale systemen

waaraan door mensen wordt deelgenomen (Gould 1997). Daarbij moet een evolutie-historische kanttekening worden geplaatst: natuurlijke selectie was er eerder dan marktwerking. Met andere woorden: natuurlijke selectie brengt niet alleen marktwerking in sociale systemen voort, zij vormt daarvan tevens weer een bestanddeel. Natuurlijke selectie heeft geleid (en leidt nog steeds) tot succesvolle soorten én tot succesvolle soorten van sociale systemen, en marktwerking heeft geleid (en leidt nog steeds) tot succesvolle soorten entrepreneurs en soorten van instituties.

Werkhypothese 1: Instituties zijn succesvol, naarmate interne veranderingen hen beter in staat stelt externe veranderingen te overleven.

Als institutie is Secure Haven succesvol wanneer deze zo flexibel is, dat het externe veranderingen kan overleven.

4.2.4 Overleven

Overleven heeft in deze zin twee kanten, een interne en een externe.

Interne krachten kunnen een institutie om zeep helpen wanneer de deelnemers eraan geen meerwaarde ervaren door hun deelname en hun belangstelling verliezen, vertrekken, of in verzet komen. Redenen zijn wanbeheer, corruptie, machtsmisbruik en dergelijke, en/of een gebrek aan doeltreffendheid, bezien vanuit de deelnemer. Instituties zijn levende systemen die worden samengesteld uit deelnemende individuen die aan het resulterende collectief voordeel ervaren (in de geest van Coase (1937), terwijl Frey (1997) heeft laten zien dat waarden hier niet alleen economisch van aard hoeven zijn). Ze vallen uiteen wanneer de waarden-calculus van de deelnemers omtrent deelname voor hen negatief uitvalt. Succesvolle instituties beschikken over de informatie en de flexibiliteit die nodig zijn om dergelijke gevaren het hoofd te bieden.

Externe krachten kunnen een institutie om zeep helpen, wanneer alternatieven beter en aantrekkelijker zijn (ze worden verdrongen) of wanneer ze worden geconfronteerd met krachten die erop gericht zijn of het effect hebben dat de institutie wordt vernietigd. Ook hier geldt dat succesvolle instituties beschikken over de informatie en de flexibiliteit die toereikend zijn om dergelijke gevaren het hoofd te bieden.

Voor een institutie als Secure Haven betekent dit dat, om succesvol te zijn, in haar structuur de *mogelijkheden* van adequate vormen van flexibiliteit moeten worden ingebouwd.

4.2.5 Flexibiliteit en maakbaarheid

Een en ander houdt in dat succesvolle instituties niet alleen structuur en vastigheid bieden die wordt verbonden met regulering en *planning*, maar eveneens de *vrijheid* moeten laten voor de verandering ervan – ook op het niveau van de individuele deelnemers en in zijn extreme vorm wordt aangeduid met een houding van *laisser faire*. Het streven naar regulering en *planning* enerzijds en naar ruimte voor *laisser faire* anderzijds komt onvermijdelijk in botsing en is een van de meest persistente argumenten bij politieke discussie binnen (Foley 2006) en conflicten tussen recht-systemen (Bobbitt 2002).

4.2.6 Wederkerigheidfalen

In de economie wordt – in deze geest – doorgaans de vrijheid van economisch transigeren een noodzakelijke voorwaarde gevonden voor de zegeningen van de marktwerking, en wordt aan de behoefte aan planning en regulering (waaraan immers ook risico's zijn verbonden, zie Teulings e.a. 2005) pas toegegeven wanneer er sprake is van marktfalen.

Die figuur, het inzetten van regulering ter bestrijding van marktfalen acht ik analoog van toepassing wanneer naast economische ook andere waarden (bijvoorbeeld de waarden van veiligheid in de openbare ruimte, van privacy, van het kunnen uiten en nastreven van idealen) bij eerdergenoemde waarden-calculus worden betrokken. Deze, gegeneraliseerde versie van 'marktwerking' noem ik 'transactiewerking,' omdat aan de basis van marktwerking de aanname ligt van individuele *economische* transacties tussen rationele individuele partijen (en niet zonder reden, zie Myerson 1997). 'Marktwerking' wordt 'transactiewerking' wanneer we het vereiste loslaten dat de transacties economisch van aard zijn. Juristen noemen dergelijke transacties overeenkomsten. 'Marktfalen' wordt alsdan 'wederkerigheidfalen' omdat – kort door de bocht – overeenkomsten van nature gebaseerd zijn op wilsovereenstemming tussen de partijen, hetgeen wederkerigheid inhoudt, die

aangeeft dat beide partijen zich bewust zijn van de toegevoegde waarden die een overeenkomst hen over en weer biedt.

De vrije ruimte voor het aangaan van overeenkomsten is in deze redenering een noodzakelijke voorwaarde voor het succes van instituties (ook van Secure Haven) omdat in die ruimte op individueel niveau de aanpassingen kunnen worden verwezenlijkt die nodig zijn om als institutie te kunnen overleven in een wijzigende leefomgeving.

Maar de hier besproken flexibiliteit is vluchtig en kan niet worden opgevat als een analogon voor de rol die mutaties van genetisch materiaal speelt in Darwin (1859).

4.2.7 *De 'genen' van instituties*

Wat zijn dan wél de 'genen' van instituties? Een bekend citaat van Oliver Wendell Holmes Jr. Geeft een indicatie:

“Law reflects and at the same time determines the fate and worth of our society [...] Like the grub that prepares a chamber for the winged thing it never has seen but is to be, we labor within our forms of constitutional decision to bring into being a just society.”⁴⁴

Het citaat roept het vermoeden op dat een bijzondere, doorgaans tamelijk stabiele en onveranderlijke verzameling regels de rol speelt van 'constitutie' voor een recht-systeem.⁴⁵ Constituties gaan over de interne organisatie van de (publiekrechtelijke) elites van een recht-systeem, over hun taken en bevoegdheden, over de begrenzing van hun bevoegdheden jegens de deelnemers en over de wijze waarop die regels kunnen worden gewijzigd. De constitutie bepaalt de 'soort' van een recht-systeem. De wijze waarop die kan worden gewijzigd onder druk van wijzigingen in de omgeving bepaalt de kans op overleving van de soort. De wijze waarop die aanpassingen *de facto* worden vormgegeven bepaalt de kans op overleven door het individuele recht-systeem. Recente, opzichtige voorbeelden van deze 'struggle for life' van recht-systemen zijn te herkennen in 'die Wende' van 1989, in de constitutionele onzekerheden die de interne organisatie en de externe betrekkingen van Israël en Palistina kenmerken en in de wisselende beoordelingen van *Guantanamo Bay* als níet (Bush) of wél (Obama) in strijd met de Amerikaanse constitutie. Kennelijk is het – ook afgezien van de onvoorspelbaarheid van wijzigingen in de omgeving – op orde houden van een constitutie niet eenvoudig als die wijzigingen tot het bewustzijn van recht-systemen doordringen. Het is opnieuw Oliver Wendell Holmes Jr. die een aanwijzing geeft over het waarom:

“A very common phenomenon, and one very familiar to the student of history, is this. The customs, beliefs or needs of primitive time establish a rule or formula. In the course of centuries the custom, belief or necessity disappears, but the rule remains. The reason which gave rise to the rule has been forgotten, and ingenious minds set themselves to inquire how it is to be accounted for. Some ground of policy is thought of, which seems to explain it and to reconcile it with the present state of things; and then the rule adapts itself to the new reasons which have been found for it, and enters upon a new career. The old form receives a new content, and in time even the form modifies itself to fit the meaning which it has received.”⁴⁶

Voor de overlevingskansen van Secure Haven houdt dit in dat er een constitutie moet zijn (anders is het helemaal geen recht-systeem) die organisatie, bevoegdheden en beperkingen van bestuurlijke elites regelt en aangeeft hoe de constitutie kan worden gewijzigd wanneer daarvoor aanleiding is door veranderingen van de omgeving.

4.2.8 *De leefomgeving van recht-systemen*

Een belangrijk verschil tussen de natuurlijke selectie van soorten en de transactiewerking die aan de basis van het overleven van recht-systemen wordt gedacht is daarin gelegen, dat rationele actoren niet alleen in staat moeten worden geacht hun eigen structuur aan te passen, maar ook hun omgeving. Er bestaat, bijvoorbeeld, een sterk vermoeden dat menselijk handelen inmiddels een de belangrijkste oorzaak is voor verande-

⁴⁴ O.W. Holmes as cited by P. Bobbitt (1983).

⁴⁵ Ik gebruik verder de term 'recht-systeem' waar ik eerder 'institutie' hanteerde.

⁴⁶ O.W. Holmes, [1881] (1968), *The Common Law*, ed. M. DeWolfe Howe, as cited by S. Deakin, ESRC Centre for Business Research, University of Cambridge Working Paper No. 203.

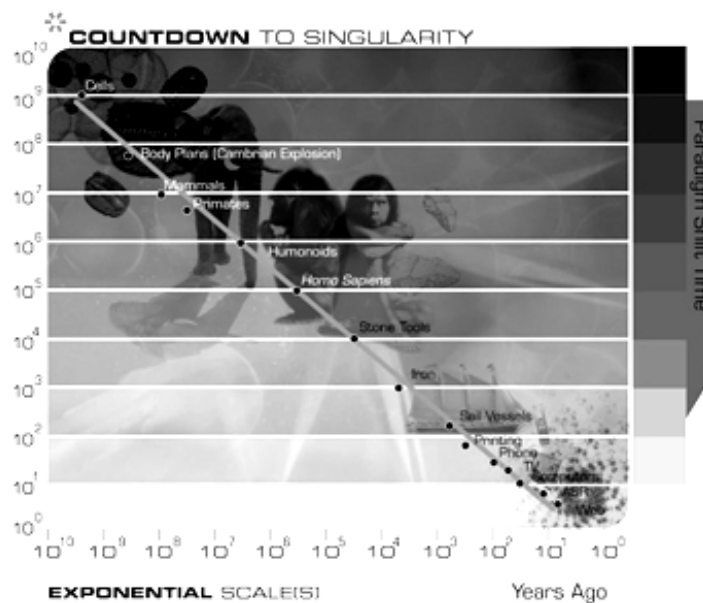
ringen van de omgeving van soorten, en, daarmee, een van de belangrijkste oorzaken voor evolutionaire verandering (Palumbi 2001). Ik acht het aannemelijk dat dergelijke ontwikkelingen ook voor Secure Haven van doorslaggevend belang zullen blijken. Ik geef hieronder een lang citaat uit Schmidt (2009), waarin ik een belangrijk argument over de invloed van te verwachten technische ontwikkelingen (Kurzweil 2001) bespreek vanuit de mogelijke invloed ervan op de rechtspraak (e-justice).

“Discussions on e-justice are often in two completely different keys. On the one hand a euphoric tone may be struck when predicting how ICT-services will help improve our adjudicatory systems while on the other hand a more reluctant tone can be heard, pointing at the risks that automation will bring to the art and culture of classic adjudication arrangements. It is indeed remarkable how euphoric one can get about automation in general. Ray Kurzweil provides an extreme example. He suggests the “singularity point” to be near. What does he mean?

Kurzweil’s argument is founded on two observations. The first one plots the percentage of people, using inventions (electricity, telephone, radio, television, mobile phone and internet respectively) against time (roughly from 1860 to 2000) in order to show that mass use of inventions is growing exponentially and has almost reached the point of full saturation. The second observes an exponential acceleration of ‘paradigm shifts’ in history. I let Kurzweil explain the paradigm-shift observation himself:

“The paradigm shift rate (i.e., the overall rate of technical progress) is currently doubling (approximately) every decade; that is, paradigm shift times are halving every decade (and the rate of acceleration is itself growing exponentially). So, the technological progress in the twenty-first century will be equivalent to what would require (in the linear view) on the order of 200 centuries. In contrast, the twentieth century saw only about 25 years of progress (again at today’s rate of progress) since we have been speeding up to current rates. So the twenty-first century will see almost a thousand times greater technological change than its predecessor.” [Kurzweil 2004]

Kurzweil illustrates this observation with the sheet in Figure 2. Figure 1 plots paradigm shifts (“technical progress”) using two identical exponential time scales. If I understand correctly, the first is used to express the intervals between the occurrences of paradigm shifts (paradigm shift time). The second one is used to order these paradigm shifts as moments in history (years ago).⁴⁷



⁴⁷ I must confess that my reading of the axes in Figure 2 must be confused, as the first one mentioned is redundant once we employ the second. If my reading were right, all paradigm-shift points would land exactly on the plotted line. As some of these points are slightly off, I must miss something. What I am missing does sadly not become clear from Kurzweil’s explanation.

Figure 2: Kurzweil's countdown to singularity

In Kurzweil's interpretation of Figure 1 the exponential acceleration of paradigm shifts is of great importance.

"If we examine the timing of these steps, we see that the process has continuously accelerated. The evolution of life forms required billions of years for the first steps (e.g., primitive cells); later on progress accelerated. During the Cambrian explosion, major paradigm shifts took only tens of millions of years. Later on, Humanoids developed over a period of millions of years, and Homo sapiens over a period of only hundreds of thousands of years.

With the advent of a technology-creating species, the exponential pace became too fast for evolution through DNA-guided protein synthesis and moved on to human-created technology. Technology goes beyond mere tool making; it is a process of creating ever more powerful technology using the tools from the previous round of innovation. In this way, human technology is distinguished from the tool making of other species. There is a record of each stage of technology, and each new stage of technology builds on the order of the previous stage." [Kurzweil 2004]

Apparently, considering the background illustrations in the upper half of Figure 2, Kurzweil has found inspiration in Darwin (1859). Nevertheless, his main point is depicted by the vortex in the lower right corner of Figure 2. This is the singularity point, the point where paradigm-shifts get so densely compressed in time, that we will no longer be able to cope and will have to accept that the products of artificial intelligence, combined with nanotechnology will take over in a world we no longer understand. The next species Kurzweil envisages is an in principle immortal, enhanced concoction of mixed artificial intelligence and nanotechnology, based on an exhaustive scan of an individual's nervous system. The new species may be brought to life by gradually replacing parts of the human beings that are to be transformed into it. The best the remaining⁴⁸ mere humans may then hope for is that their species will be tolerated by the next after it has taken over. One cannot but wonder what will happen to e-justice after the singularity point has arrived. One of its first quests will be to decide on who will be immortalized and who will not.

Considering Kurzweil's rather considerable techno-optimism, I would expect him to predict that his new 'species' will be organized under some extreme high-quality form of e-justice, although he is not very clear about it where it matters. What he *is* clear about are the dangers that accompany technological paradigm shifts that are meant for the good, yet may be employed for the bad. Past, current and future examples are technical paradigm shifts allowing for kaleidoscopic threats to realize, e.g., chemical, nuclear and biological warfare, global heating, computer virus attacks and terrorist actions deploying self-reproducing nanobots. I do not share Kurzweil's optimism, as I do not see how the extreme high-quality form of global e-justice required will emerge from first copying current humane intelligence and subsequently let it improve itself. There are real threats in technological progress and in the ways we may employ its results.

One of the most amazing aspects of [Kurzweil 2004] is its complete blind spot for law systems as significant environments to how inventions will be used. Another surprise is Kurzweil's use of 'paradigm shift,' embodying both significant DNA-mutations *and* moments of significant technical progress, thus blurring the connotations of both concepts. I simply find it very hard to stomach humans with- and humans without a particular batch of new inventions as different *species*. And I find it excessively romantic (Mary Shelly-like) rather than scientific to consider the immortal bionic man to represent a species at all.

Nevertheless, I partially agree with Kurzweil's argument. Technical progress is accelerating exponentially indeed, and, with it, the threat-rate of mass-destructive abuse is accelerating towards quite another singularity point: the moment that a single individual will be capable to mass-destruct its proper species on earth. Where singularity-point thinking leads to fantasies about turning some of us into immortal bionic men with superhuman intelligence, I loose interest. Where singularity-point thinking

⁴⁸ As this process when available must be quite costly and not available to all, selecting who may and who may not be converted into an instance of the immortal 'next' species must be considered to belong to the class of tragic choices.

leads to worries about a world wherein a, any, single individual is capable of mass destruction, I do not. Assuming the president of the United States of America to be one of the few individuals who currently have mass-destructive capabilities, we hope (sometimes in vain, though) that the law guides his decisions. We may need to rethink our legal arrangements however when mass-destructive capabilities get randomly proliferated over individuals. When the enormity of the risks involved requires proactive enforcement (including surveillance), we may even need to turn to quite comprehensive e-justice services in order to survive.”

Van belang in deze blik op de toekomst voor Secure Haven is de verwachting dat, op vrij korte termijn, door de exponentiële groei in technologische vindingen een omgeving ontstaat waarin willekeurige individuen over instrumenten voor massavernietiging beschikken en dat de vraag aandacht verdient hoe Secure Haven onder die omstandigheid zal kunnen overleven. Antwoorden op die vraag zijn in het voorafgaande rapport voorbereid.

4.2.9 *Puurheid en gevaar, framing en moral panics*

Het veranderen van constituties van recht-systemen naar aanleiding van veranderingen in de leefomgeving is steeds ingebed in de communicatie tussen bestuurlijke elites en de deelnemers van recht-systemen. In de sociale wetenschappen is daarbij onderkend hoe belangrijk de rol is die wordt gespeeld door communicatietechnieken. Twee ervan zijn van bijzondere betekenis: *framing* (bijvoorbeeld: Gitlin 1980) en de opwekking en verwerking van *moral panics* (bijvoorbeeld: Cohen 1972, zie echter ook de vorige paragraaf).

Genoemde technieken worden net name dan ingezet, wanneer de ‘zuiverheid’ van recht-systemen conceptueel in gevaar komt door externe invloeden (of veranderingen in de leefomgeving). Douglas (1966) inventariseerde de verschillende typen reacties die daarop in ‘primitieve’ culturen worden ontwikkeld en maakt aannemelijk dat deze nog steeds werkzaam zijn in moderne recht-systemen. Smits (2002) analyseert onze reacties op technologische innovatie vanuit de bevindingen van Douglas, en komt tot aanbevelingen.

Omdat deze technieken wereldwijd gemeen goed zijn in politieke processen en veelvuldig worden ingezet om waarheid-vijandige argumenten door te drukken kan kennis ervan op brede schaal bijdragen aan het succes van recht-systemen. In de voorafgaande rapportage is aan deze technieken geen aandacht besteed.

4.2.10 *Verantwoording van de LRE-methode*

Hét bezwaar vanuit de *mainstream* rechtstheorie tegen benaderingen als die van LRE, die voor de rechtswetenschap analogieën zien met de biologie, de economie en de sociale wetenschappen is erin gelegen dat LRE niet de norm centraal stelt, maar de structuur, de flexibiliteit, de leefomgeving en het overlevingsvermogen van instituties of recht-systemen. Vanuit de LRE-benadering is het zoeken naar een ‘Grundnorm’ een zinloze onderneming omdat die er niet is. Normen zijn (in de zin van het tweede citaat van Oliver Wendell Holmes Jr. hierboven) voor LRE regels die in de praktijk zijn ontstaan als gevolg van de verschillende manieren waarop verschillende recht-systemen onder verschillende externe omstandigheden hun overlevingsstrategieën hebben ingericht. Wanneer die omstandigheden het noodzakelijk maken voor overleving van zowel individu als recht-systeem dat bij het aangaan van overeenkomsten rekening wordt gehouden met de belangen van beide partijen, dat ligt het voor de hand dat zulks in constitutionele regels wordt vastgelegd. Wanneer dat niet (meer) zo is, dan ligt het vanuit LRE-optiek voor de hand dat een dergelijke regel *de jure* of *de facto* wordt losgelaten, zoals de recente geschiedenis overigens veelvuldig laat zien. Onze moraliteit kan op deze wijze empirisch worden gefundeerd en aan gezag winnen in vergelijking met een fundering op opinie, op individuele overtuiging. Radbruch (1946) kan ook op die manier worden begrepen.

LRE is ontleend aan de inspanningen die in de informatica zijn verricht naar aanleiding van wat daar de *software crisis* werd genoemd (de periode waarin grote aantallen ICT-systemen niet levensvatbaar bleken of niet konden overleven), in samenhang met de aanvaarding van de analogieën die bestaan tussen het inrichten en onderhouden van ICT-diensten en het inrichten en onderhouden van recht-systemen. LRE is *work in progress*, dat nader onderzoek kan velen. In de rapportage kwam aan de orde dat de bevindingen van LRE voor Secure Haven voor de hand lijken te liggen. Ik zie daarin vooralsnog geen aanleiding de benadering te verwerpen.

Aangehaalde literatuur

G. A. Akerlof (1970),

The Market for 'Lemons': Quality Uncertainty and the Market Mechanism, *Quarterly Journal of Economics* 84 488--500

P. Bobbitt (1982),

Constitutional Fate: Theory of the Constitution

P. Bobbitt (2002),

The Shield of Achilles: War, Peace, and the Course of History

R. H. Coase (1937),

The Nature of the Firm, *Economica* 4 386-405

S. Cohen (1972),

Folk devils and moral panics

C.H. Darwin (1859),

On the Origin of Species by Means of Natural Selection or, The Preservation of Favoured Races in the Struggle for Life

M. Douglas (1966),

Purity and Danger: an Analysis of the Concept of Pollution and Taboo

M. Douglas (1986),

How Institutions Think

D.K. Foley (2006),

Adam's Fallacy – A Guide to Economic Theology

L. L. Fuller (1967),

The Morality of Law, revised edition

B. S. Frey (1997),

Not Just For the Money: an Economic Theory of Motivation

T. Gitlin (1980),

The Whole World is Watching: Mass Media in the Making and Unmaking of the Left

S. J. Gould (1997),

Darwinian Fundamentalism, *The New York Review of Books* 44 (10)

A. Greif (2006),

Institutions and the Path to the Modern Economy: Lessons from Medieval Trade

R. Kurzweil (2001),

Law of Accelerating returns (Lifeboat Foundation Special Report
<http://lifeboat.com/ex/law.of.accelerating.returns>, downloaded on February 28, 2009)

L. Lessig (1999),

Code and Other Laws of Cyberspace

Montesquieu (J. de Secondat) (1748)

De l'Esprit des Lois

R. B. Myerson (1999),

Nash Equilibrium and the History of Economic Theory, *Journal of Economic Literature* XXXVII
1067-1082

R. B. Myerson (2007),

Perspectives on Mechanism Design in Economic Theory ([http:// nobel-
prize.org/nobel_prizes/economics/laureates/2007/myerson_ lecture.pdf](http://nobel-prize.org/nobel_prizes/economics/laureates/2007/myerson_lecture.pdf))

D. North (1990),

Institutions, Institutional Change and Economic Performance

M. Olson (2000),

Power and Prosperity: Outgrowing communist and capitalist dictatorships

S.R. Palumbi (2001),

Humans as the World's Greatest Evolutionary Force, *Science* 239, p. 1786-1790

G. Radbruch (1946),

Statutory Lawlessness and Supra-Statutory Law, *Oxford Journal of Legal Studies* 26 (2006) 1-11

A. Smith (1776),

An Inquiry into the Nature and Causes of the Wealth of Nations

A. H.J. Schmidt (1985),

Spaghettiwetgeving in wetsontwerp 18 764, *Delikt en Delinkwent* 15 (3) 181-188

A. H.J. Schmidt (2004),

Bedreigen computers ons rechtssysteem?

A.H.J. Schmidt (2007),

IT and the judiciary in the Netherlands – A state of affairs, *Computer Law & Security Report* 23
453-460

A.H.J. Schmidt (2009),

Radbruch in Cyberspace: about law-system quality and ICT innovation, thans bij de uitgever

G. Schreiber and others (2000),

Knowledge Engineering and Management: The CommonKADS Methodology

M. Smits (2002),

Monsterbezwinging - de culturele domesticatie van nieuwe technologie

B. Z. Tamanaha (2004),

On the Rule of Law

C.N. Teulings, A.L. Bovenberg and H. van Dale (2005),

De cirkel van goede intenties: de economie van het publiek belang

R. Tilman (2002)

Durkheim and Veblen on the Social Nature of Individualism, *Journal of Economic Issues*, 36

T. Veblen (1898)

Why is Economics not an evolutionary Science, *The Quarterly Journal of Economics*, 12

R. J. Wieringa (1997),

Requirements Engineering: Frameworks for Understanding

O. E. Williamson (2005),

The Economics of Governance. *American Economic Review* 95

I. Wright (1973),

Functions, *Philosophical Review* 82 139-168