EBB notitie

TNO 2016 R10347

Beveiligen zonder Hinder: operationalisatie van een complex begrip

Datum	6 januari 2016
Auteur(s)	Jeroen van Rest
Aantal pagina's	37 (incl. bijlagen)
Programmanaam	Experimenteeromgeving Bewaken & Beveiligen (EBB)
TNO locatie	Oude Waalsdorperweg 63, 2597 AK Den Haag
Website	www.tno.nl

POLITIE Koninklijke Marechaussee TNO innovation for life

Inhoudsopgave

1 Inleiding

Het programma Experimenteeromgeving Bewaken en Beveiligen beoogt een effectievere en efficiëntere werkwijze te ontwikkelen voor de taak ‘bewaken en beveiligen’ van de KMar, Nationale Politie en NCTV. Met behulp van de methodiek *Concept Development & Experimentation* (CD&E) wordt de werkwijze vormgegeven, en worden coherente deelconcepten (*bouwstenen)* in experimenten getest. De innovaties die in de bouwstenen worden voorgesteld, kunnen uiteindelijk worden ingevoerd in de nieuwe werkwijze (De Jong, Kwaijtaal, Verkoeijen, & Weima, 2011).

Eén van deze bouwstenen is *Beveiligen zonder Hinder*. Het doel van deze bouwsteen is om een coherent concept te beproeven waarmee de hinder ten gevolge van beveiliging voor beveiligden en hun omgeving zo laag mogelijk is, bij gelijkblijvende of verhoogde veiligheid.

Zowel veiligheid als hinder zijn complexe begrippen, waardoor het ook lastig is om daar kwantitatief (“zo laag mogelijk”, “gelijkblijvend”, “verhoogd”) mee om te gaan. Ook zijn er de subjectieve veiligheid en hinder, die afhankelijk zijn van individuele en sociale factoren, en die dus voor iedereen verschillen.

1.1 Probleemstelling

Het doel van beveiliging is om een te beschermen persoon, object of proces (het te beveiligen belang, TBB) te beschermen tegen bepaalde externe opzettelijke dreigingen. Diegenen die belast zijn met die beveiliging moeten daarom informatie verzamelen over zowel het TBB, over zichzelf, en over mogelijke dreigingen in de omgeving. Met behulp van deze informatie moeten zij voorkomen dat de dreiging zich bij het TBB manifesteert. Dat kan door tijdig te interveniëren op de dreiging, door bepaalde kwetsbaarheden in het beveiligingssysteem af te sluiten, of door het TBB uit de gevaarlijke situatie weg te halen. Om te verzekeren dat hier voldoende tijd voor is, kunnen vertragende barrières worden gebruikt. Beveiliging bestaat dus uit:

- informatie verzamelen en verwerken,
- vertragen, en
- interveniëren (Garcia, 2007).

Ieder van deze functies zijn in potentie een bron van hinder voor beveiligden en hun omgeving. De uitdaging van beveiligen zonder hinder is dus het minimaliseren van de hinder vanuit deze beveiligingsfuncties voor vriendelijke personen, terwijl de beveiligingsfunctie optimaal blijft.

De scope van dit onderzoeksprogramma is objectbeveiliging ten dienste van het beschermen van Te Beschermen Personen (TBP’s), zodat zij op die objecten de persoonsbeveiliging niet meer nodig hebben. Aangezien de nabijheid van persoonsbeveiliging ook als een bron van hinder kan worden gezien, kan worden beargumenteerd dat alles dat bedraagt aan het veiliger maken van het object ook bijdraagt aan het reduceren van hinder.

Hinder en veiligheid kunnen per onderdeel van een beveiligingsconcept worden beschouwd, zoals per beveiligingsmaatregel, werkproces of –in het geval van dit onderzoeksprogramma- per bouwsteen. Echter, de uiteindelijke (objectieve en subjectieve) veiligheid en hinder zijn het resultaat van het geheel aan maatregelen, in hun samenhang. De begrippen moeten dus concrete betekenis krijgen die eensluidend is over de gehele experimenteeromgeving, het toepassingsgebied van objectbeveiliging en het aanpalende toepassingsgebied van persoonsbeveiliging. Het concept veiligheid is in diverse studies en (beleids)documenten al nader omschreven, maar het concept hinder niet. Een gevolg hiervan is dat er nog maar erg weinig wetenschappelijk onderzoek is gedaan wat mensen nu daadwerkelijk aan hinder ondervinden: er is immers nog geen model van hinder waarbinnen eventuele bevindingen geplaatst kunnen worden.

In de experimenteeromgeving is het een randvoorwaarde dat er gebruik wordt gemaakt van kennis en technologie “van de plank”. In dit geval is de operationalisatie van hinder dus nog niet beschikbaar.

1.2 Doel van deze memo

Het doel van deze memo is om:

1. Het begrip hinder, zoals te gebruiken in Experimenteeromgeving Bewaken & Beveiligen, nader te duiden –te operationaliseren- aan de hand van bestaande beleidsdocumenten, literatuur en voorbeelden.
2. Aan de hand van die duiding een voorstel te doen voor een model voor de beleving van hinder, waarmee de te verwachten hinder voorspeld kan worden.
3. Aan de hand van die duiding en dat model hinder concreet te maken voor de experimenteeromgeving, en dus uit te werken voor de relevante bouwstenen.

1.3 Scope, randvoorwaarden en uitgangspunten

Deze memo beperkt zich tot hinder die veroorzaakt wordt door beveiligingsmaatregelen en de wijze van beveiliging, en die ervaren wordt door de te beveiligde persoon (TBP) en zijn sociale omgeving, waaronder ook mogelijke tegenstanders (hierna: subjecten, personen en doelgroepen). Dat zijn bijvoorbeeld aangebrachte technische-, bouwkundige maatregelen, zoals een sluis of slagboom, of een slot op een raam.

Hinder direct veroorzaakt door de dreiging waartegen beveiligd wordt, valt buiten de scope van deze memo.

Hinder door beveiligingsmaatregelen die alleen ervaren wordt bij het bedienen van die maatregelen door beveiligingspersoneel scharen we onder *(on)werkbaarheid* en valt buiten de scope van deze memo. Een voorbeeld daarvan is loze alarmen.

Er zijn diverse mogelijke bronnen van hinder. Velen liggen echter niet in de directe invloedssfeer van beveiligers en bewakers. Bijvoorbeeld, bouwvakkers die in de

buurt van een beveiligde woning aan het heien zijn, kunnen een bron van geluidshinder zijn, maar dit heeft niet direct iets met beveiliging van doen. Het valt dus buiten de scope van deze memo.

Beveiliging zelf kan op allerlei manieren hinder veroorzaken, bijvoorbeeld als beveiligers zwerfafval op het terrein zouden achterlaten tijdens surveillancerondes. Deze memo beperkt zich echter tot hinder die intrinsiek het gevolg is van beveiliging. Hinder, mogelijk veroorzaakt door beveiliging, maar die daar niet intrinsiek bij hoort, valt dus ook buiten de scope van deze memo.

Het installeren, onderhouden en weer weghalen van beveiligingsmaatregelen kan ook hinder opleveren. Dergelijke hinder is echter niet specifiek voor beveiligingsmaatregelen, en valt om die reden dus ook buiten de scope van deze memo.

Een beveiligd persoon kan de hinder voor zijn sociale omgeving willen verkleinen door zijn vrienden en familie op afstand te houden gedurende de periode dat hij in beveiliging zit. Dat kan ook weer hinder opleveren. Deze memo is echter beperkt tot de hinder die direct vanuit beveiligingsmaatregelen uit gaat. Andere indirecte effecten op de TBP, zoals een eventueel verhoogd gevoel van status, vallen ook buiten de scope van deze memo.

1.4 Leeswijzer

In hoofdstuk 2 wordt het begrip hinder nader geduid aan de hand van literatuur en beleidsdocumenten. In hoofdstuk 3 wordt hinder per bouwsteen uitgewerkt. De psychosociale gevolgen van hinder worden uitvoerig beschreven in (Nijdam, Olff, Vries, Martens, & Gersons, 2008). In hoofdstuk 4 wordt beschreven hoe bepaalde aanbevelingen uit dat rapport in de Experimenteeromgeving opgepakt zouden kunnen worden. In hoofdstuk 5 wordt de hindermatrix geïntroduceerd. In hoofdstuk 6 wordt beschreven hoe in het onderzoeksprogramma de hinder in een aantal bouwstenen wordt verminderd. Hoofdstuk 7 beschrijft hoe het combineren van diverse deelconcepten kan helpen om de hinder nog verder te verminderen. In hoofdstuk 8 worden de conclusies en enkele aanbevelingen gegeven.

1.5 Dankwoord

De ideeën die in deze memo staan verwoord, zijn tot stand gekomen uit interactie met de volgende personen: Fred van Puffelen, Eric van Santen, Folkert Roosjen, Albert Nieuwenhuijs en Graeme van Voorthuijsen.

2 Context

Bij het operationaliseren van hinder is het van belang om rekening te houden met de juridische en maatschappelijke context.

2.1 Juridisch kader

De beleving van hinder en service (zie ook sectie 3.8) wordt mede beïnvloed door de perceptie van legitimiteit van beveiligingsmaatregelen (Van der Kleij, Roelofs, & Van Hemert, Gaan veiligheidsmaatregelen ten koste van de servicebeleving?, 2015). Als beveiligingsmaatregelen illegaal zijn, dan is er over het algemeen weinig steun voor. Een gebrek aan acceptatie voor een maatregel hoeft dus niet (alleen) aan de ervaren hinder te liggen. Het juridisch kader –en de kennis daarvan bij mensen die mogelijk hinder ondergaan- is dus relevant.

Beveiliging van personen en objecten wordt vaak gedaan om mensen te beschermen. Het Europese Verdrag voor de Rechten van de Mens (EVRM) bevat bijvoorbeeld:

- artikel 2: het recht op leven,
- artikel 5: recht op vrijheid en veiligheid, en
- artikel 8: Recht op eerbiediging van privé-, familie- en gezinsleven.

Het wrange van beveiliging is nu juist dat op dergelijke artikelen uitzonderingen moeten worden gemaakt om ze te kunnen handhaven:

- op Artikel 2: omdat uiteindelijk een tegenstander kan worden omgebracht als het onmiddellijke risico voor de beveiligde maar groot genoeg is,
- op Artikel 5: omdat een tegenstander kan worden vastgezet als hij een gevaar vormt voor een beveiligd persoon of object,
- op Artikel 8: omdat privacy-invasieve beveiligingsmaatregelen kunnen worden genomen.

Het EVRM is uitgewerkt in meer specifieke wetten. Ambassades vallen bijvoorbeeld onder artikel 22, lid 2 van het Verdrag van Wenen inzake diplomatiek verkeer:

> "*Op de ontvangende staat rust de bijzondere verplichting alle geëigende maatregelen te nemen om de gebouwen van de zending tegen indringers en tegen het toebrengen van schade te beschermen en te verhinderen dat de rust van de zending op enigerlei wijze wordt verstoord of aan haar waardigheid afbreuk wordt gedaan.*"

2.2 Maatschappelijke context

De hinder van beveiliging heeft ook maatschappelijke impact. Het wordt gezien als een noodzakelijk kwaad dat veroorzaakt wordt door de dreiging. Als publieke personen worden bedreigd, dan kan de hinder van beveiliging hun publieke functioneren beïnvloeden. Het kan zelfs voorkomen dat de hinder die bekende personen van beveiliging ondergaan als een soort martelaarschap worden

neergezet. Hierdoor vereist de beveiliging van dergelijke personen extra tact en integriteit.

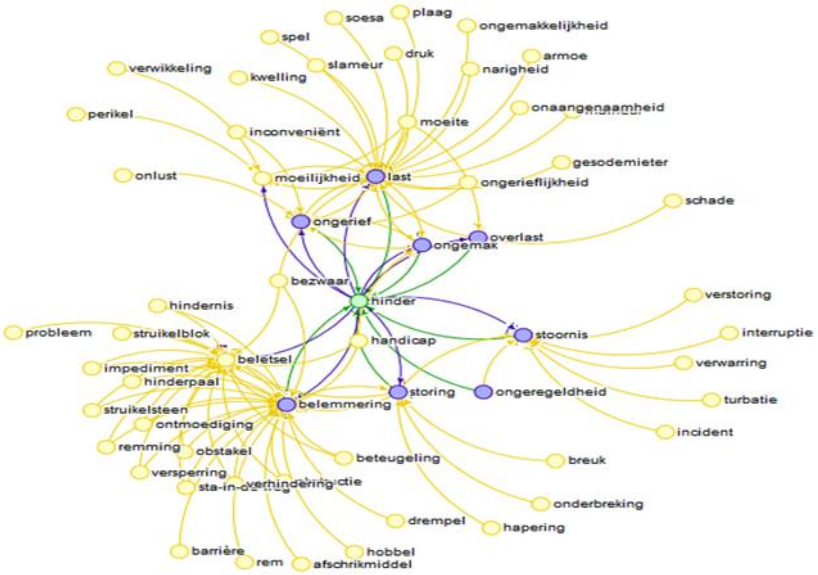
Door concrete aanvallen of aanslagen –en de daaropvolgende berichtgeving– kunnen aangebrachte beveiligingsmiddel(en) maatschappelijk gezien meer geaccepteerd worden. De keerzijde daarvan kan optreden wanneer de feitelijke dreiging verdwenen is, maar de maatschappelijke –of politieke– angst er nog wel is. De beveiliger kan dan worden ingezet om “voor de bühne” wel te blijven beveiligen –en hinderen– terwijl dit dus objectief bezien niet meer nodig is.

3 Hinder

Hinder is een complex begrip. In dit hoofdstuk wordt daarom eerst de betekenis van het woord “hinder“ en enkele verwante begrippen behandeld. Daarna wordt beschreven wat de mogelijke effecten van hinder zijn, inclusief het nut dat door goed toegepaste hinder ervaren kan worden.

3.1 Betekenis van hinder

Hinder betekent: overlast, het last hebben van iets. Het engelse *hindrance* betekent iets dat het moeilijker maakt voor je om iets te doen, of om iets te ontwikkelen. In Figuur 1 zijn een aantal gerelateerde termen gevisualiseerd die kunnen helpen om in een gesprek alert te zijn op tekenen van hinder.



Figuur 1 Woordverbanden van "hinder". (bron: Synoniemen.net)

Hinder wordt ervaren door een natuurlijk persoon. Als er geen sprake is van een natuurlijk persoon, dan is er dus ook geen hinder. In de context van bewaken & beveiligen zijn er allerlei personen die mogelijk hinder ervaren. In eerste instantie zijn er de beveiligde en zijn directe sociale omgeving, zijn familie, vrienden en collega’s. Dan zijn er ook omwonenden en andere mensen in de directe omgeving, waaronder ook het (beveiligings)personeel. En ook de tegenstander kan hinder ervaren.

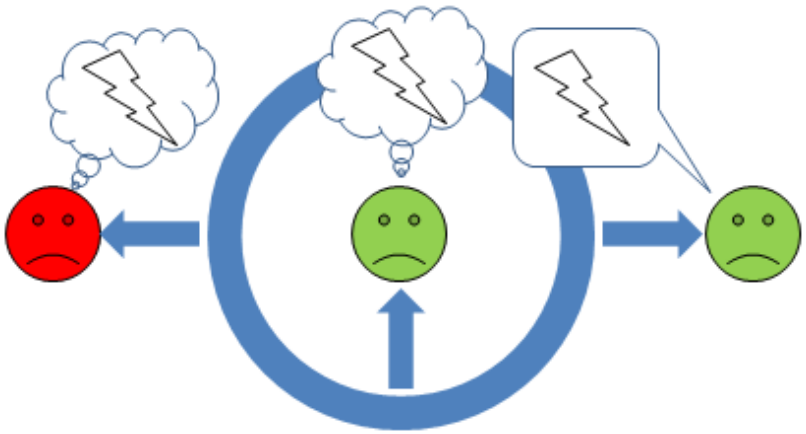
3.2 Oorzaken voor, en effecten van hinder

Het is dus mogelijk om een causale keten te beschreven van hinder door beveiliging:

1. Een beveiligingsmaatregel heeft een werking (informatie verzamelen, vertragen en/of interveniëren).

2. Deze werking heeft ook een bijwerking, namelijk de beleving van diverse vormen van hinder. Dit maakt de beveiligingsmaatregel een bron van hinder.
3. De beleving van hinder heeft zelf ook weer andere effecten. Deze 2e orde effecten kunnen positief en negatief gewaardeerd worden.

In de volgende paragrafen worden achtereenvolgens hinderbronnen, de focus van hinder, soorten hinder, directe en indirecte hinder, en de effecten van hinder behandeld. In Figuur 2 worden de eerste drie daarvan gevisualiseerd.



Figuur 2 De beveiliging die om de beveiligde heen staat (de blauwe ring), levert hinder op voor (van links naar rechts) de dreiging, de beveiligde en zijn naasten. De beveiligde kan ook meevoelen met de hinder die (middels de blauwe pijlen) door zijn sociale omgeving wordt gevoeld.

3.3 Hinderbronnen

Hinder heeft altijd een bron. In de context van bewaken en beveiligen zijn er minstens twee mogelijke bronnen van hinder: de dreiging, en de beveiligingsmaatregelen. Deze komen bovenop de reguliere hinder die men in het normale sociale verkeer van alle dag ondervindt: een verkeersfile, luidruchtige buren, een oude sportblessure die opspeelt of erger. Een enkele hinderbron kan op meerdere manieren hinder opleveren. Een toegangscontrolesysteem kan bijvoorbeeld zowel hinderlijk zijn omdat er persoonsgegevens (bijv. biometrie) worden geregistreerd, omdat er gewacht moet worden tot het systeem de deur open doet, en omdat er eens in de zoveel keren een (ongewenst) alarm af gaat waar de beveiliging op af komt. Paragraaf 3.5 gaat verder in op de verschillende wijzen waarop hinderbronnen bij een persoon tot hinder kunnen leiden.

Er kan ook tegelijkertijd sprake zijn van meerdere hinderbronnen. Het kan zo zijn dat meerdere hinderbronnen elkaar tijdelijk en/ of lokaal onderdrukken of juist versterken. Dit kan zowel objectief als subjectief. Bijvoorbeeld, de aanwezigheid van een hinderlijke fan kan voor een TBP maken dat een normaal hinderlijke toegangscontrole op die plek tijdelijk als zeer prettig wordt ervaren. Het wegnemen van een hinderbron (de toegangscontrole) hoeft dus niet altijd te leiden tot minder hinder, en de aanwezigheid van een extra hinderbron (de fan) kan de aandacht

althans op korte termijn soms afleiden van andere hinder. Hiermee wordt niet gepleit voor het introduceren van afleidingen om de subjectieve hinder maar zo laag mogelijk te laten zijn, maar wel voor een beter begrip en daarmee acceptatie voor wisselende waarderingen van hinder door TBP's en andere betrokkenen.

Maar er kunnen ook andere effecten optreden tussen verschillende hinderbronnen dan afleiding. Bijvoorbeeld kan men hinder ervaren als er een discrepantie tussen dreiging en beveiliging wordt ervaren: beveiligingsmaatregelen die niet lijken te passen bij de dreiging, of andersom, dreiging waar de beveiligingsmaatregelen niet bij lijken te passen.

Hinderbronnen kunnen ook in de persoon zelf gelegen zijn. Een persoon kan zichzelf hinderen, bijvoorbeeld als hij met zichzelf in conflict is. Iemand kan bijvoorbeeld een functie hebben gekregen die hij jarenlang heeft geambieerd en waar hijzelf en zijn familie veel voor hebben opgeofferd. Ook wist hij dat er continu een bepaalde dreiging op de functie zit. Echter, in de praktijk valt het leven onder dreiging en beveiliging hem toch te zwaar. Normaal gesproken zou hij stoppen met zijn functie, maar de verwachtingen uit zijn sociale omgeving kunnen een interne conflictsituatie opleveren die kan leiden tot stress die hem hindert in zijn functioneren.

3.4 Focus van hinder

Hinder kan een algemeen, ongerichte ervaring zijn, in de zin van "last hebben", maar ze kan ook bedoeld worden in betekenis van "last hebben bij …". Dan gaat het meer om een verstoring of onderbreking van een (werk)proces. In het plaatje met woordverbanden in Figuur 1 zijn bovenin de niet-gefocuste vormen van hinder te herkennen, en onderin de meer gefocuste vormen.

De constante aanwezigheid van andere mensen in de nabijheid, zoals beveiligers of mede-beveiligden, kan een algemene beleving (i.e. niet-gefocuste vorm) van hinder beïnvloeden. Sommige mensen kunnen zich dan bijvoorbeeld niet volledig ontspannen, wat op den duur kan leiden tot vermoeidheid. Een toegangscontrole die een onderbreking vormt bij het betreden van een pand kan daarnaast juist een meer gefocuste hinder opleveren bij een proces zoals het betreden van een pand, zoals een vertraging, of een aantal handelingen die moet worden voltooid.

Om de gevolgen van gefocuste hinder te verminderen kan het helpen om de beveiligingsmaatregelen zo goed mogelijk te laten aansluiten bij het reguliere proces van de TBP. Gebruik bijvoorbeeld vertragende maatregelen op momenten dat de TBP toch al ergens anders ook op moet wachten.

In deze memo worden beide soorten focus van hinder meegenomen: de later voorgestelde operationalisatie van hinder kan zowel gefocuste als niet-gefocuste hinder beschrijven. Daarvoor is het eerst nodig om te verkennen hoe hinderbronnen zoals die in beveiliging te vinden zijn, leiden tot de beleving van hinder, zowel gefocust als niet-gefocust.

3.5 Directe en indirecte hinder

Het is mogelijk dat de persoon zelf geen directe hinder ondervindt (of hij accepteert deze), maar wel hinder voelt omdat zijn familie of vrienden wel direct hinder ervaren. In dit rapport wordt dit “indirecte hinder” genoemd. Daarmee kan het onderscheid worden gemaakt tussen direct zelf ervaren hinder, en indirect meegevoelde hinder.

Deze indirecte hinder kan bijvoorbeeld de achtergrond zijn waartegen een beveiligd persoon zichzelf (tijdelijk) kan willen verwijderen van zijn naasten. Hiermee verkleint hij de hinder van de dreiging en beveiliging voor hen, en daarmee verkleint hij voor zichzelf een deel van de meegevoelde hinder. Het kan natuurlijk ook nog gebeuren, dat de persoon juist directe en indirecte hinder ervaart als de afstand tot familie en vrienden door dergelijke ingrepen te groot wordt. Hieruit kan geleerd worden dat er ook nog andersoortige directe hinder van belang kan zijn dan die direct vanuit beveiligingsmaatregelen wordt ervaren. Dit rapport is beperkt tot hinder die direct door beveiligingsmaatregelen wordt veroorzaakt.

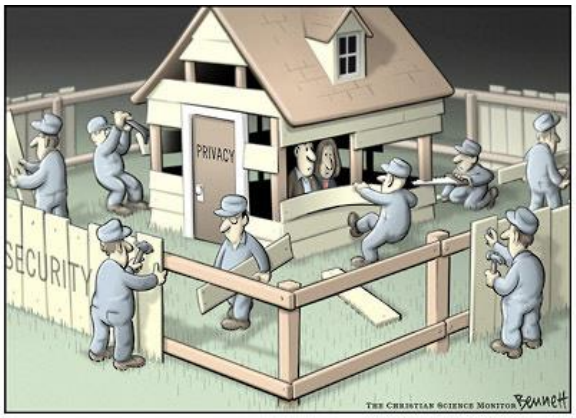
3.6 Hoe leidt beveiliging tot de beleving van directe hinder?

Er zijn verschillende manieren waarop een hinderbron bij een persoon leidt tot directe hinder. Zoals in de probleemstelling reeds is benoemd, de soorten hinderbronnen die intrinsiek zijn aan beveiligingsmaatregelen zijn beperkt tot:

- informatie verzamelen en verwerken,
- vertragen, en
- interveniëren [2].

Het is dus de uitdaging om een kader te vinden dat het verband legt tussen mogelijke bronnen van directe hinder in de omgeving van een persoon enerzijds, en de ervaren directe hinder door de persoon anderzijds. Dat kader moet het verband kunnen leggen tussen enerzijds de drie mogelijke soorten hinderbronnen vanuit beveiliging, en anderzijds een logische verklaring kunnen geven voor de interne beleving door de persoon. Ook moet dat kader een kwantitatief karakter hebben om te kunnen redeneren over meer en minder hinder.

In deze paragraaf wordt beschreven in hoeverre de concepten *privacy, invasiviteit* en *keuzevrijheid* dat kader zouden kunnen bieden.



Figuur 3 Beveiliging ten koste van privacy. (Bron: ClayBennett.com)

In de volgende drie paragrafen wordt beargumenteerd dat deze drie concepten alle verschillende soorten hinder afdekken die een persoon zelf van beveiligings-maatregelen kan ervaren. In hoofdstuk 5 wordt deze argumentatie gebruikt om een *hindermatrix* voor te stellen, een categorisering van de verschillende soorten hinder die beveiligingsmaatregelen kunnen opleveren.

3.6.1 Privacy als denkkader voor de reden waarom mensen directe hinder ervaren

Er zijn verschillende soorten privacy, zoals bescherming van persoonlijke gegevens, bescherming tegen fysieke indringing in de persoonlijke ruimte, en de bescherming om zelfstandig beslissingen te kunnen nemen (Langheinrich, 2001) (Solove, 2006). Wetenschappelijke literatuur is echter niet eenduidig over welke soorten privacy er zijn, of hoe ze zich tot elkaar verhouden (Van Rest, Everts, Van Rijn, & Van Paassen, 2012). In Tabel 1 wordt dit geïllustreerd aan de hand van verschillende beveiligingsmaatregelen als mogelijke hinderbronnen voor de privacy van doelgroepen. Hierin wordt geen onderscheid gemaakt tussen beveiligden, omstanders of tegenstanders.

Tabel 1 Verschillende soorten privacy geïllustreerd aan de hand van beveiligingsfuncties en –maatregelen. Solove's *Information dissemination* heeft geen relatie met de drie kerntaken van beveiliging, dus die is weggelaten.

Beveiligingstaken en voorbeelden van maatregelen als hinderbronnen		**Solove[1]**			**Langheinrich**					
		Invasions	**Collection**	**Processing**	**Territory**	**Person (bodily)**	**Personal behaviour (media)**	**Personal communications (interception)**	**Personal data**	**# deelconcepten**
Informatie verzamelen en verwerken	Surveilleren middels CCTV	X	X	X	X		X		X	7
	Post openen	X	X	X			X	X	X	
Vertragen	Hek	X			X		X			3
Interveniëren	Aanhouden	X			X	X	X			4

[1] Solove heeft ook een vierde groep privacy invasieve activiteiten benoemd: dissemination. Het verder verspreiden van informatie heeft geen relatie met beveiliging, dus die groep is in deze tabel niet opgenomen.

Het concept privacy heeft echter geen duidelijk kwantitatief element. Dat zou kunnen worden geïntroduceerd door te turven hoeveel soorten privacy worden aangetast per soort beveiligingsmaatregelen, op een 3-dimensionale schaal van respectievelijk 7, 3 en 4 punten.

3.6.2 Invasiviteit als denkkader voor de reden waarom mensen directe hinder ervaren

Het deelconcept “invasions” van Solove beschrijft een groep invasieve activiteiten die niet perse met het verzamelen van informatie te maken hebben. Daaronder vallen ook activiteiten die de rust van een individu verstoren, en die de beslissingsvrijheid verkleinen. In zijn woorden:

> *“The fourth and final group of activities involves invasions into people’s private affairs. Invasion, unlike the other groupings, need not involve personal information (although in numerous instances, it does). Intrusion concerns invasive acts that disturb one’s tranquillity or solitude. Decisional interference involves the government’s incursion into the data subject’s decisions regarding her private affairs.”* (Solove, 2006)

In eerder onderzoek is ook verkend hoe het begrip *invasiviteit* in het maatschappelijk en wetenschappelijk discours wordt gebruikt (Van Rest, Roelofs, & Van Nunen, Afwijkend Gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid–tweede herziene druk. No. TNO 2014 R10987., 2014). Daar zijn vijf verschillende soorten gebruik verzameld, zie Tabel 2.

Tabel 2 Varianten van het gebruik van invasiviteit

Soort invasiviteit	Voorbeeld uit beveiliging
Verlies van autonomie	Interveniëren, vertragende middelen
Vastleggen informatie	Surveillance
Bijvangst	Vastleggen van beelden van voorbijgangers
Gebrek aan legitimiteit	Spionage
Gebrek aan kenbaarheid	Heimelijke observatie

De eerste twee soorten invasiviteit (verlies van autonomie en vastleggen van informatie) zijn in dat rapport ook nader uitgewerkt in schalen van invasiviteit waarmee de mate invasiviteit van concrete beveiligingsmaatregelen beschreven kan worden. Ook deze kunnen worden geïllustreerd aan de hand van beveiligingsmaatregelen, zie Tabel 3.

Tabel 3 Het concept invasiviteit toegepast op soorten beveiligingsmaatregelen. X = van toepassing. # = Van toepassing en er is een schaal voor.

	Voorbeeld	Verlies van autonomie	Vastleggen van informatie	Bijvangst	Gebrek aan legitimiteit	Gebrek aan kenbaarheid	# deelconcepten
Informatie verzamelen en verwerken	Surveilleren middels CCTV of post openen		#	X	X	X	4
Vertragen	Hek	#		X	X	X	4
Interveniëren	Aanhouden	#		X	X	X	4

Het kwantitatieve element zou ook hier kunnen worden geïntroduceerd door te turven hoeveel soorten invasiviteit er van toepassing zijn per soort beveiligings-maatregelen, op een 3-dimensionale schaal van ieder 4 punten.

3.6.3 Keuzevrijheid als denkkader voor de reden waarom mensen hinder ervaren

Zoals reeds genoemd, één van de vormen van privacy is de bescherming van keuzevrijheid. Vooral in de filosofie is daar veel aandacht aan besteedt. In een recent toegankelijk artikel over dat onderwerp wordt het “Freedom quotient” (FQ) voorgesteld, equivalent aan het Intelligentie Quotient en het Emotie Quotient (Cave, 2015). Het FQ van een persoon wordt door drie factoren bepaald:

- de vaardigheid om opties te creëren,
- de vaardigheid om te kiezen, en
- de vaardigheid om één op meerdere van die opties te realiseren.

Als één van deze vaardigheden beperkt is, dan is de redenering van dit artikel dat dan de keuzevrijheid van de persoon is ingeperkt.

Het FQ kan ook op beveiliging worden toegepast. Om te beginnen is beveiliging bedoeld om opties realiseerbaar te houden, namelijk om bepaalde dingen te doen die anders door de dreiging onmogelijk worden gemaakt. Echter, aan de andere kant maakt beveiliging helaas ook bepaalde opties onmogelijk doordat de beveiligingsmaatregelen ook ruimte, geld en aandacht vragen. (Object)beveiliging heeft dus vooral invloed op de keuzevrijheid met betrekking tot het *realiseren* van opties.

3.7 Effecten van hinder: nut en last

Hinder (vanuit beveiliging) kan tot verschillende effecten leiden, afhankelijk van wie de hinder ondervindt. In deze paragraaf wordt voor de eenvoud alleen onderscheid gemaakt tussen beveiligden, omstanders en tegenstanders, maar in de praktijk kan het nuttig zijn om onderscheid te maken tussen principalen, hun directe familie en nabije vrienden, vast personeel, leveranciers, etc. Bij tegenstanders kan nader onderscheid worden gemaakt in verschillende dreigingen, bijv. journalisten, stalkers, gelegenheidsdieven en terroristen.

Hinder kan leiden tot een gebrek aan draagvlak voor de beveiliging bij de beveiligden, zeker als het hun normale functioneren beïnvloedt. Dit kan leiden tot klachten bij beveiligingsinstanties, en in het uiterste geval tot het zich onttrekken aan beveiliging of het ontvluchten van de situatie(s) (bijv. een functie op het werk) waar de dreiging op gericht is. Beveiliging die tot hinder leidt bij omstanders kan leiden tot antipathie t.o.v. de beveiligde, wat bij de beveiligde tot meevoelende hinder kan leiden. Ook zij kunnen klagen bij de beveiligingsinstanties. In uiterste gevallen kan hinder leiden tot gerichte sabotageacties.

Hoofdstuk 4 gaat uitvoerig in op de psychosociale effecten van hinder, aan de hand van (Nijdam, Olff, Vries, Martens, & Gersons, 2008).

Over het algemeen wordt het als positief beschouwd als tegenstanders hinder ondervinden. De vertragingstijd die een barrière oplevert kan door de beveiliging gebruikt worden om de tegenstander te neutraliseren of de beveiligde te evacueren. Ook kan hinder als afschrikkingsmiddel gebruikt worden. Een toegangscontrole die strenger werkt voor personen die in het verleden hebben laten zien dat ze zich minder goed aan de huisregels houden, kan mogelijk ook een afschrikwekkend effect hebben[2]. Een uiterste geval hiervan is “show the force”. Een nadeel van hinder bij de tegenstander is dat de beveiliging niet meer heimelijk kan gebeuren.

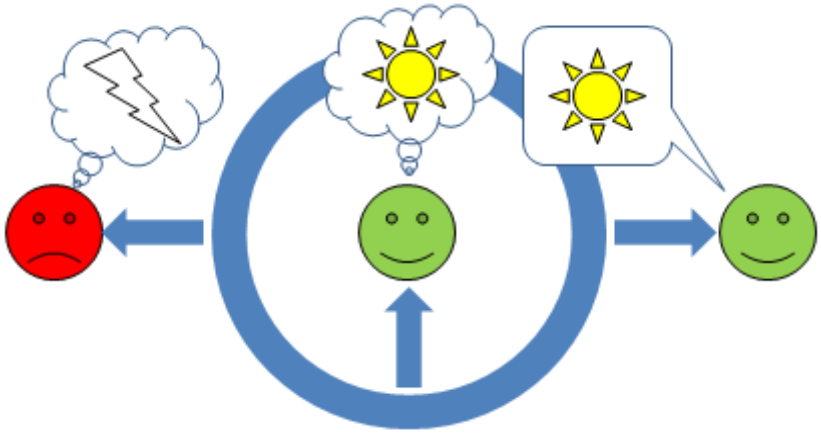
Echter, erg hinderlijke beveiliging kan ook weerstand oproepen in die mate dat neutrale of zelfs vriendelijke personen geprikkeld worden om een meer vijandige attitude te ontwikkelen ten opzichte van de beveiliging, of zelfs ten opzichte van het te beveiligen belang. Het is dus ook verstandig om althans een idee op te bouwen van de mate van hinder voor (potentiele) tegenstanders.

Hinder kan ook statusverhogend werken. Dat kan in bepaalde gevallen nuttig zijn.

3.8 Hinder en service

Het tegenovergestelde van hinder is service: het actief ondersteunen van iemand in zijn behoeften. Het verschil tussen hinder en service kan zeer subjectief zijn. Het welkom heten van iemand bij het binnenkomen van een receptie, kan op een neutrale omstander als service overkomen, terwijl het door een tegenstander als hinderlijk kan worden ervaren.

[2] Dit is het idee achter de wijze waarop bij ADO Den Haag wordt omgegaan met de threshold van de gezichtsherkenning bij de toegangscontrole.



Figuur 4 Service als veiligheidsmaatregel kan een middel zijn om beveiligden en hun naasten minder hinder te laten ondervinden bij gelijkblijvende veiligheid, mits die service een beveiligingsfunctie uitoefent richting de dreiging.

Veiligheid en service liggen dicht bij elkaar[3]. Veiligheid betekent o.a. dat de normale gang van zaken door kan blijven gaan, en service is het helpen van anderen bij hun normale gang van zaken. Veiligheid is dus randvoorwaardelijk voor service, en andersom kan service gebruikt worden om veiligheid te creëren. Dat kan ook te ver gaan als het leveren van service er toe leidt dat de beveiligingsfunctie in het gedrang komt. Boodschappen doen voor een beveiligd persoon is dus niet aan de orde, tenzij daarmee een risico wordt verkleind.

[3] Security as a Service (SaaS) is echter weer een heel ander begrip. Daar gaat het om het leveren van diensten die tot veiligheid leiden, zoals een surveillancedienst, in tegenstelling tot alleen het leveren van beveiligingsmiddelen zoals personeel en camera's.

4 Psychosociale gevolgen van dreiging en beveiliging

De NCTV heeft eerder onderzoek laten doen naar de psychosociale gevolgen van dreiging en beveiliging. Hierbij is gefocust op de psychologie van de beveiligde persoon en zijn directe sociale omgeving, zie ook Figuur 5.

Figuur 5 Dreiging, persoonsbeveiliging en gevolgen voor de taakuitvoering en het privéleven (Nijdam, Olff, Vries, Martens, & Gersons, 2008).

Het rapport van dit onderzoek eindigt met enkele tientallen aanbevelingen welke mede richtinggevend kunnen zijn voor het onderzoek in de Experimenteer-omgeving. Sommige aanbevelingen zijn concreet en direct bruikbaar, en kunnen dus direct opgenomen worden in de Concept of Operations. In de volgende paragrafen worden enkele relevante (delen van) aanbevelingen geciteerd die wel meer uitwerking vereisen. Per aanbeveling wordt een reflectie gegeven van de mogelijke consequenties voor de bouwstenen van de Experimenteeromgeving en / of de werkprocessen van de ConOps (Peters & De Groen, 2015). De titels van de paragrafen komen overeen met de titels van de respectievelijk aanbevelingen in dat rapport.

4.1 Beveiligde personen betrekken bij het te voeren beveiligingsbeleid

> *Het zou goed zijn de 'sense of control' van bedreigden te versterken door meer informatie te verstrekken en hier ook in de beveiliging meer aandacht aan te besteden. Nadrukkelijk wordt niet gepleit voor een 'u vraagt, wij draaien' opzet, maar wel voor betrokkenheid bij de te nemen cruciale beslissingen, die immers het leven van bedreigden betreffen. […] Tegelijkertijd moet ook steeds duidelijk gemaakt kunnen worden dat niet alle gevoelige informatie ter beschikking gesteld kan worden.*

Het gaat hier om "deels geïnformeerd" meebeslissen over de eigen beveiliging. Wellicht kan de objectieve hinder per beveiligingsmaatregel worden beschreven, zonder daarbij te veel gevoelige informatie ter beschikking te stellen. Kan een te

beveiligen persoon daarmee zinvol meebeslissen bij het maken van het beveiligingsplan?

4.2 Systematische evaluatie van psychosociale aspecten van beveiliging en adviesgesprekken

> *Een logische volgende stap is om met behulp van vragenlijsten, evaluaties en eventueel onderzoek naar psychobiologische parameters meer zicht te krijgen op de tot nu toe gepresenteerde thema's en effecten. Aan de hand van dit soort onderzoek kan specifieker gekeken worden naar psychosociale effecten van beveiliging.*

De subjectieve (ervaren) hinder kan vergeleken worden met de objectieve hinder. Eventuele verschillen kunnen vervolgens aan omgevings- en psychobiologische parameters toegewezen worden. Met deze kennis kan –eventueel ook zonder direct meebeslissen door te beveiligen personen- de hoeveelheid ervaren hinder verminderd worden.

4.3 Beginfase

> *Voor een goede relatie tussen de beveiligde en beveiligers is het van belang dat vooraf voor iedereen duidelijk is waar de grenzen liggen in wat men van de beveiliging mag verwachten.*

Voor wat betreft de verwachting van de grenzen aan hinder, deze kunnen wellicht meer concreet worden beschreven. De hinder bij de toegangscontrole zou bijvoorbeeld beperkt kunnen worden binnen een beperkte wachttijd.

4.4 Interactie tussen beveiligers en beveiligden

> *Met het aspect afstand/nabijheid wordt door de beveiligers verschillend omgegaan, hetgeen kan leiden tot spanningen met de beveiligde en tussen de beveiligers onderling.*

Afstand tot een persoon kan wellicht uitgedrukt worden in een mate van hinder. Dit past bijvoorbeeld bij ideeën over invasiviteit.

> *Bij het nemen van beveiligingsmaatregelen wordt aangeraden de beveiligde een zekere mate van keuzevrijheid te bieden, zodat een bepaalde mate van controlebehoud ervaren wordt.*

Deze aanbeveling lijkt goed te passen bij de eerdere aanbeveling van paragraaf 4.1.

4.5 Informatievoorziening

> *Volgens de beveiligers kunnen zij niet over alle informatie beschikken om hun werk goed te kunnen doen. Dit kan een gevoel van controleverlies geven. Aanbevolen wordt om de procedure van interne informatievoorziening binnen de DKDB* (dit heet tegenwoordig de DBB) *te evalueren en te communiceren.*

De Experimenteeromgeving heeft verschillende experimenten die hier op in spelen, zoals in de bouwsteen Actueel Veiligheidsbeeld.

> *Het verstrekken van informatie aan de beveiligde over de beveiligingsmaatregelen en de dreiging zal vaak leiden tot stressreductie. Er kan echter een spanningsveld bestaan tussen de informatiebehoefte van de beveiligde en de door de beveiligers verstrekte informatie. Geadviseerd wordt deze informatie zoveel mogelijk te geven. Hierbij dient men er rekening mee te houden dat de informatiebehoefte voor iedere persoon verschillend is en afhangt van de stijl van informatieverwerking.*

Door specifieker te kunnen zijn in informatie apart over hinder, zonder daarbij ook alles over de beveiligingsmaatregelen te moeten vertellen, kan er wellicht een groter deel van de informatiebehoefte van beveiligden worden ingevuld.

4.6 Opleiding en training

> *De procedures die gebruikt worden in een crisissituatie worden niet daadwerkelijk geoefend met de beveiligden of op een andere manier met hen doorgenomen. Door dit tot op zekere hoogte wel te doen op bijvoorbeeld een trainingsdag of door filmmateriaal hierover met hen door te nemen, zullen de beveiligden adequater kunnen reageren en zullen de gevoelens van onveiligheid afnemen.*

In de experimenteeromgeving zit een bouwsteen Real Life Training. Daarin is expliciet besloten om de te beveiligen persoon niet bij deze vorm van training te betrekken vanwege het voorkomen van hinder. In het licht van bovenstaand advies zou hier in specifieke gevallen van afgeweken kunnen worden.

> *Volgens de beveiligers wordt er tijdens hun opleiding nauwelijks aandacht besteed aan de psychosociale aspecten van de beveiliging. In de opleiding tot beveiliger zou er tijd en aandacht moeten worden ingeruimd voor de interactie met de beveiligde, de impact van de beveiliging op de beveiligde, stress en stressmanagement en een training in sociale vaardigheden.*

Onder de noemer real life training zouden beveiligers ook te maken kunnen krijgen met beveiligden (“red team”?) die specifieke behoeften hebben op het gebied van hinder.

5 Hindermatrix

Het is in de experimenteeromgeving nodig om vast te kunnen stellen of innovaties leiden tot meer of juist minder hinder. Daarom moet hinder geoperationaliseerd worden. Hiertoe wordt in dit hoofdstuk de ‘hindermatrix’ voorgesteld.

Deze operationalisering kan gebruikt worden in combinatie met de aanpak zoals beschreven in het vorige hoofdstuk over de psychosociale gevolgen van hinder (Nijdam, Olff, Vries, Martens, & Gersons, 2008). Het gebruik van de hindermatrix moet niet in de plaats komen van die aanpak.

5.1 Functie van de hindermatrix

Op basis van de hindermatrix kan van te voren een concrete en complete inschatting worden gemaakt van de directe hinder die beveiligingsmaatregelen opleveren. Dit inzicht kan daarmee bijvoorbeeld in een vroeg stadium worden gedeeld met de beveiligde, zonder daarbij inzage te hoeven hebben in gevoelige informatie over de dreiging of beveiligingsfunctionaliteit. Ook kan aangegeven worden welke mate van hinder ervaren, gewenst, toegestaan, verwacht of geaccepteerd is.

Een hindermatrix is slechts bedoeld als een benadering, een model, van de complexe juridische kaders en psychologische processen die tezamen bepalen welke hinder een persoon[4] echt ervaart. Naarmate het model nauwkeuriger is, zal het de ervaren hinder beter voorspellen. Maar, een complexer model is weer minder begrijpelijk en werkbaar in de praktijk. Als zodanig is het in deze memo ook slechts bedoeld als hulpmiddel om zo goed mogelijk met hinder om te gaan, en niet als wetenschappelijk kader om de werkelijkheid mee te bestuderen.

5.2 Wat is de hindermatrix

Een hindermatrix legt dus een verband tussen beveiligingsmaatregelen enerzijds, en objectieve maten voor hinder anderzijds. In paragraaf 3.6 zijn drie denkkaders verkend: privacy, invasiviteit en keuzevrijheid. Op basis daarvan wordt bij deze voorgesteld om per beveiligingsmaatregel de volgende criteria als indicatoren voor hinder vast te leggen:

1. De mate van detail van informatie
2. De gemiddelde vertraging (tijd)
3. De mate van verlies van autonomie

Criteria 1 en 3 zijn de mate van invasiviteit zoals beschreven in paragraaf 6.4.1 van (Van Rest, Roelofs, & Van Nunen, Afwijkend Gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid–tweede herziene druk. No. TNO 2014 R10987., 2014). Deze drie criteria dekken de drie functies van beveiliging af volgens de volgende tabel.

[4] Zowel te beveiligen persoon, zijn sociale omgeving, als tegenstanders.

Tabel 4 Dekking van beveiligingsfuncties door voorgestelde maten van hinder.

Eenheid	Detail van informatie Schaal van 0-6	Vertraging Tijd	Verlies van autonomie Schaal van 0-6
Informatie verzamelen	X		
Vertraging		X	X
Interveniëren		X	X

De “score” op deze drie maten kan verschillen per type gebruiker. De twee – dimensionale hindermatrix kan dus worden uitgebreid met een derde dimensie die varieert per gebruikersgroep. Dat wordt duidelijk gemaakt in de volgende paragraaf over use cases.

5.3 Use cases van de hindermatrix

De criteria dienen gespecificeerd worden voor verschillende doelgroepen, zoals de beveiligde zelf, zijn naasten of juist de tegenstander, of eventueel nog specifieker. Afhankelijk van de werking van beveiligingsmaatregelen, ervaren deze doelgroepen immers verschillende *use cases*, met dus ook verschillende vormen van hinder.

De hindermatrix is ook bruikbaar voor samengestelde beveiligingsconcepten, of voor compartimenten binnen een groter beveiligd object. Daarbij gelden de volgende regels. Vertraging is cumulatief en moet dus worden opgeteld. Voor de criteria voor invasiviteit (verlies van autonomie, detail van informatie) moet het maximum worden genomen.

Tabel 5 Voorbeeld van een hindermatrix: de directe hinder van verschillende vormen van authenticatie voor toegangscontrole bij de betreding van een compartiment voor doelgroepen die recht hebben op toegang.

	Vertraging	Verlies van autonomie[5]	Detail van informatie5
Pas aanmelden bij betreding van ieder compartiment	5 sec	4	2
Biometrie aanbieden bij betreding van ieder compartiment	5 sec	4	2
Biometrie-op-afstand bij betreding van ieder compartiment	0 sec	2	2

[5] De criteria “verlies van autonomie” en “detail van informatie” en 3 zijn de mate van invasiviteit zoals beschreven in paragraaf 6.4.1 van (Van Rest, Roelofs, & Van Nunen, Afwijkend Gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid–tweede herziene druk. No. TNO 2014 R10987., 2014).

5.4 Het nut van de hindermatrix tegen psychosociale gevolgen van dreiging en beveiliging

In het vorige hoofdstuk worden in paragrafen 4.1 tot 4.6 een aantal vragen opgeworpen met betrekking tot de psychosociale gevolgen van dreiging en beveiliging. In deze deelparagraaf wordt beschreven hoe de hindermatrix daarbij kan helpen.

De hindermatrix kan helpen om een TBP zinvol te laten meebeslissen, of althans te informeren bij het maken en uitvoeren van het beveiligingsplan. De kolom met specifieke beveiligingsmaatregelen kan bijvoorbeeld vanwege veiligheid niet worden getoond aan de TBP, en de hinderfactoren wel.

De antwoorden van vragenlijsten en evaluaties kunnen worden vergeleken met de objectieve directe hinder. Op basis daarvan kan worden onderzocht welke soorten TBP's gevoelig zijn voor welke soorten objectieve directe hinder.

De hindermatrix kan gebruikt worden om de grenzen van de opgelegde hinder van te voren duidelijk te omschrijven.

Het aspect afstand / nabijheid van beveiligers is een specifieke bron van hinder (autonomie: 2 en informatie: 3 volgens de schaal van de hindermatrix). Het kan helpen om met beveiligers afspraken te maken over of ze in het zicht zijn van de TBP enerzijds, of de mate waarin ze de TBP zijn gang laten gaan. Daarnaast kan er op de beveiligde objecten technologie worden toegepast waardoor de beveiligers minder fysiek in de buurt hoeven te zijn. Zie daarvoor hoofdstukken 6 en 7 van deze memo.

Door (de theorieën achter) de hindermatrix ook een onderdeel te laten zijn van de opleiding van beveiligers, kunnen zij zelfstandig beter rekening houden met dit aspect.

6 Hinder per bouwsteen

In de experimenteeromgeving kan deze matrix gebruikt worden om eventuele gevolgen voor hinder van een aantal verschillende deelconcepten -de bouwstenen- te duiden. Dat wordt in deze paragraaf gedaan voor de volgende bouwstenen:

- Actueel veiligheidsbeeld: PSIM en mobiel
- Schaalbaar en effectief interveniëren
- Intelligente dreigingsdetectie: prikkelen
- Persoon begeleidingssysteem
- Beveiligen zonder hinder: hindermatrix
- Beveiligen zonder hinder: screenen van voertuigen
- Interactieve informatiegestuurde toegangsregulering

Daarnaast is het mogelijk om vanuit het werkproces zelf een “satéprikker” door een aantal bouwstenen heen te steken en te beschrijven hoe –althans in theorie– verschillende bouwstenen elkaar kunnen versterken om op die manier de hinder te verminderen. Dat wordt in het volgende hoofdstuk beschreven.

In deze memo wordt uitgegaan van de beoogde werking, dus vóórdat de uitslagen van de experimenten bekend zijn.

6.1 Beveiligen zonder hinder: hindermatrix

Op basis van de hindermatrix zoals die in deze memo is voorgesteld, is een serie gedachte-experimenten uit te voeren met beveiligers. Daarin kan worden onderzocht:

1. De werkzaamheid van de toepassing van de voorgestelde hindermatrix.
2. De mogelijke knelpunten bij het gebruik van de hindermatrix.
3. Mogelijke verbeteringen van de hindermatrix in het algemeen en eventueel ter operationalisatie in het bijzonder.

De te toetsen hypotheses zijn de volgende:

A. Het expliciteren van hinder tijdens de ontwerpfase zorgt er voor dat het resulterende beveiligingsplan minder hinder oplevert.

B. Het expliciteren van hinder tijdens de ontwerpfase zorgt er voor dat de TBP de beveiliging meer accepteert.

6.2 Schaalbaar en effectief interveniëren

In de praktijk van het bewaken en beveiligen van hoog-risico objecten zijn er altijd meerdere organisaties betrokken bij de beveiliging. Bij sommige objecten van het Koninklijk Huis bijvoorbeeld de DBB, de KMar en politie eenheid Den Haag. De beveiligingsplannen worden echter doorgaans door de verschillende ketenpartners separaat opgesteld. Dit brengt risico’s met zich mee; niet alleen voor wat betreft de effectiviteit en efficiency van de beveiliging, maar ook ten aanzien van de

schaalbaarheid. Interventies kunnen effectiever en efficiënter worden uitgevoerd als duidelijke afspraken vooraf worden gemaakt. Afstemming van afspraken tussen ketenpartners is hierin van groot belang.

Om deze afstemming te bevorderen is er voor het experiment 'schaalbaar en effectief interveniëren een concept ontwikkeld waarmee de verschillende partijen samen een integraal beveiligingsplan kunnen maken. Centraal in het concept voor schaalbaar en effectief interveniëren staat een multi-user software applicatie, bij de Nationale Politie ook wel bekend als iTable (De Jong & Vullings, 2014). De tool is bedoeld om door de betrokken diensten gezamenlijk te gebruiken. Juist de gezamenlijke 'situational awareness' die hierdoor ontstaat, leidt naar verwachting tot integrale inzetconcepten, i.e. beveiligingsplannen die beter op elkaar zijn afgestemd en daarmee effectiever zijn (Hogeweg, Van den Brekel, Vullings, Hasberg, & Van Rest, 2015).

Eén van de hypotheses die ten grondslag liggen aan het experiment is dat het gebruik van de iTable leidt tot een beter inzicht in de effecten van beveiligingsmaatregelen. Als de hinder dus ook wordt geëxpliciteerd, dan zou het kunnen dat dit tot minder hinder leidt, net zoals dit bij het experiment met de hindermatrix zou kunnen werken.

6.3 Intelligente dreigingsdetectie: prikkelen

Het doel van het experiment prikkelen is: "het bijdragen aan het palet van oefenmogelijkheden bewaken & beveiligen op gebied van 'prikkelen' ". Dit wordt gedaan door het ontwikkelen en uitproberen van een proof-of-concept training met daarin een verdieping van de kennis van prikkelen (Van der Kleij, Wijn, & Van Rest, Prikkelen door bewakers en beveiligers van hoog risico objecten – TNO Memo, 2015).

Als beveiligers hierdoor accurater gaan prikkelen, dan is het mogelijk dat minder personen geprikkeld worden, en er dus netto minder hinder wordt gecreëerd.

6.4 Interactieve informatie-gestuurde toegangsregulering

De bouwsteen interactieve informatie-gestuurde toegangsregulering is gericht op het voorkomen dat ongeautoriseerde personen binnen kunnen komen door pogingen daartoe tijdig te detecteren, en op het zorgen dat geautoriseerde personen wel binnen kunnen komen. Dit bij minder hinder door snellere toegang. De verwachting daarbij is dat dit gewaardeerd wordt door bezoekers en TBP's, en dat het vastleggen van meer gegevens van mensen (bijv. biometrische kenmerken) niet tot belemmeringen leidt. Ook is het de verwachting dat een snellere toegang alleen mogelijk is als het aantal handelingen dat door de persoon moet worden verricht, beperkt blijft. Het aantal handelingen zou in ieder geval ten opzichte van de huidige toegangsregulering niet moeten toenemen: dat zou leiden tot meer hinder, in plaats van minder.

De hinder die iemand bij biometrische authenticatie ondervindt wordt bepaald door meerdere factoren:

- de false non match rate bepaalt de kans dat iemand onterecht geweigerd wordt en dus opnieuw een biometrische opname moet laten maken, of naar de back-up procedure wordt doorverwezen,
- de mate waarin iemand moet meewerken voor een succesvolle biometrische opname. Als de persoon moet stoppen dan is dat meer hinder dan als hij door kan bewegen. Als de persoon een specifieke houding moet aannemen, dan is dat meer hinder dan als de houding niet uit maakt,
- de mate van detail van informatie die iemand moet afgeven voor een biometrische opname. Informatie die toch al zichtbaar is, zoals een gezicht, is minder hinderlijk dan informatie die niet zonder meer zichtbaar is, zoals iris of retina. Hersengolven zijn hier het meest invasief en dus hinderlijk,
- de vertraging die iemand oploopt door de hele toegangsprocedure.

6.5 Beveiligen zonder hinder: screenen van voertuigen

Het doel van dit experiment, het screenen van voertuigen en hun inhoud bij toegangscontrole, is om de kans te verkleinen van een aanval op een VIP in een beveiligd object (Van der Jagt, Jezierska, & Van Rest, 2015). Dit wordt gedaan door de consequenties te veranderen van een poging van een aanvaller om toegang te proberen te krijgen met een voertuigen met wapens / explosieven er in. Dit wordt bereikt door detectie, waarvan de prestatie objectief kan worden bepaald, en door afschrikwekkende werking. Het experiment gaat over detectie van wapens en explosieven in voertuigen. Eén van de hypotheses is dat het screenen van voertuigen minder hinder oplevert voor gasten.

Het feit dat bezoekers soms hun auto niet mogen meenemen binnen de beveiligde zone rondom een beveiligd object kan een bron van hinder zijn. Door auto's te screenen op wapens en explosieven kan deze bron van hinder worden weggenomen.

In Tabel 6 wordt het verschil in directe hinder beschreven die de bezoeker ervaart. Ten eerste ervaart de bezoeker minder vertraging, omdat hij zijn voertuig niet meer elders hoeft te parkeren: hij kan nu naar het vitale gebied rijden. Uiteraard is dit alleen een vermindering van een vertraging als de voettocht naar het vitaal gebied meer tijd kost dan het screenen van het voertuig (dat mogelijk tegelijk kan worden gedaan met het screenen van het persoon) plus de rit naar het vitaal gebied. Dit betekent dat deze verandering in hinder alleen kan worden gerealiseerd bij objecten met een groot beschermd gebied en / of met verafgelegen publieke parkeerruimte.

Ten tweede, de bezoeker houdt meer autonomie: hij is niet meer gedwongen om gedurende zijn gehele bezoek gescheiden te worden van zijn voertuig, alleen nog maar tijdelijk tijdens de screening.

Echter, de prijs (in termen van hinder) die moet worden betaald is het vrijgeven van bepaalde informatie: het screeningsproces zal informatie over zijn voertuig opleveren, en daarmee over hemzelf.

Voor de TBP verandert er niets aan zijn beleving van directe hinder als hij een aparte ingang gebruikt (dat wordt ook aanbevolen voor veiligheidsredenen). Hij kan echter minder *indirecte* hinder ervaren, omdat hij ziet dat zijn bezoekers minder hinder ervaren.

Tabel 6 De bezoeker ervaart verschillende soorten hinder: meer autonomie en minder vertraging, in ruil voor het prijsgeven van bepaalde informatie.

	Bezoekers voertuig wordt geweigerd	**Bezoekers voertuig wordt toegelaten na screening**
Vertraging	Meer	Minder
Informatie	Geen	Ja
Autonomie	Minder	Meer

De waardering van deze verandering in hinder is persoonlijk. Het is daarom geen onderwerp van dit experiment. In ieder geval heeft de bezoeker hiermee meer opties.

6.6 Persoon begeleidingssysteem

Het uitgangspunt voor de oplossingsrichting van deze bouwsteen is begeleiden op afstand door gebruik te maken van specifieke technologie voor de lokalisatie van de bezoeker (Van Rest, Sandbrink, & Van Voorthuijsen, Experiment Persoon Begeleidingssysteem (PB), 2015).

In meerdere opzichten kan de objectieve directe hinder daardoor minder worden, zie ook Tabel 7. Ten eerste doordat mensen meer vrijheid hebben: ze hoeven niet met een beveiliger of ander personeelslid mee te lopen; ze hoeven alleen iets bij zich te dragen. Dit leidt dus tot minder niet-gefocuste hinder. Dit werkt alleen indien bezoekers onderweg geen obstakels aantreffen (bijv. gesloten deuren waarvoor ze wel geautoriseerd zijn) die ze zelf niet open kunnen doen, en als ze goed de weg kennen of daarbij ondersteund worden. Ten tweede omdat er minder informatie van hen wordt geobserveerd. Hier moet wel de kanttekening bij worden geplaatst dat de locatie van de bezoeker over tijd wel ook persoonsgegevens kunnen zijn, en dus als zodanig behandeld moeten worden. Een valkuil, in termen van hinder, kan zijn als het aanbrengen of afdoen van de tag veel tijd kost (inclusief eventuele administratieve handelingen). Dat moet dus nadrukkelijk voorkomen worden. Er moeten dus ook voldoende tags zijn zodat bezoekers niet hoeven te wachten totdat andere bezoekers klaar zijn.

Tabel 7 De begeleiding middels technologie kan minder hinder opleveren dan begeleiding door een persoon.

Begeleiding varianten	**Vertraging**	**Autonomie**	**Informatie detail**
Begeleiding door persoon	Begeleider beschikbaar maken.	4 – vragen om gedrag	3 – reactie op prikkel
Begeleiding middels tag	Tag aanbrengen en af doen.	3 - dragend	1 – locatie (en uiterlijk)

Afhankelijke van de uitvoering heeft het gevolgen voor de werkbaarheid voor beveiligers. Wellicht moet het live gemonitord worden, en elke (ongewenste) melding moet worden gevalideerd.

6.7 Actueel veiligheidsbeeld: PSIM en Mobiel

In deze bouwsteen zijn twee experimenten uitgevoerd. Het eerste experiment werd opgezet om te toetsen of een *physical security information management* (PSIM) systeem daadwerkelijk het actueel veiligheidsbeeld kan verbeteren en of het wenselijk is om het binnen het operationele proces van KMar en Nationale Politie ten behoeve van de beveiliging van objecten in te zetten. Het PSIM systeem moet namelijk goed te gebruiken zijn voor de beveiligers, maar ook goed te integreren en te onderhouden zijn door beheerders van (IT)systemen.

Met het tweede experiment – het AV Mobiel Experiment – wordt de meerwaarde onderzocht van het uitrusten van beveiligers met mobiele apparatuur waarmee zij enerzijds directer inzicht kunnen krijgen in het AV (bijvoorbeeld de locatie van andere beveiligers, informatie over VIP's, bezoekers, of (potentiële) incidenten/verdachten) en anderzijds zelf kunnen bijdragen aan het AV door het doorsturen van informatie naar de centrale (bijvoorbeeld hun locatie, of tekst en foto's gerelateerd aan hun locatie) (Bouthoorn, et al., 2015).

Heel in het algemeen kan worden gesteld dat als beveiligers betere informatie hebben dat ze dan minder fouten maken[6]. Dat kan op diverse manieren leiden tot minder hinder. Een voorbeeld is het controleren van de identiteit bij een toegangscontrole met behulp van een mobiel device dat live bijgewerkt wordt bij wijzigingen. Ook aan bezoekers die pas zojuist geautoriseerd zijn, kan dan direct toegang worden verleend.

[6] Betere informatie kan in de praktijk ook minder informatie betekenen. Een "te goede" informatie positie kan bijvoorbeeld leiden tot te veel extra werk.

7 “*Single sign-on*” voor “*keys to the castle*”

In dit hoofdstuk wordt beschreven hoe verschillende deelconcepten uit dit onderzoeksprogramma mogelijk kunnen samenwerken om de hinder voor de TBP nog verder te beperken[7].

7.1 Context

Sommige objecten zijn dermate goed beveiligd dat de persoonsbeveiligers na aankomst op het object niet verder mee het object op hoeven te gaan. De fysieke nabijheid van de beveiligers is immers ook een bron van niet-gefocuste hinder. Bij de aankomst van een TBP op een beveiligd object kan de TBP nog wel door hen worden geauthentiseerd, zodat aan zijn aankomst geen aparte handeling of technologie te pas hoeft te komen.

7.2 Uitdaging: “keys to the castle”

Echter, ook binnen beveiligde objecten is het in principe nodig om bij iedere overgang naar een compartiment met een hoger beveiligingsniveau een authenticatiestap uit te voeren[8]. Er zijn daar bovenop ook beveiligde objecten met veel ringen of althans deelcompartimenten. In principe wordt bij het indelen daarvan rekening gehouden met de werkbaarheid voor medewerkers en / of het comfort van bewoners. Desondanks kunnen er groepen medewerkers zijn die in bepaalde delen niet mogen komen, terwijl bijvoorbeeld de TBP daar wel mag komen. Is het mogelijk om het authenticatieproces voor de TBP op dergelijke interne compartimentsgrenzen met minder hinder te laten plaatsvinden, dus zonder begeleiding door persoonsbeveiligers, maar ook zonder handelingen van de TBP?

7.3 Doel van “keys to the castle”

Het doel is dus dat eenmaal dat de TBP is geauthentiseerd, hij dat op het object niet nog een keer hoeft te doen. De hoofdingang, i.e. de overgang van het observatiegebied naar het beveiligd gebied laten we daarbij buiten beschouwing omdat we er daarbij vanuit mogen gaan dat de TBP geauthentiseerd wordt door zijn persoonsbeveiligers.

7.4 Achtergrond: single sign-on

Het principe dat een gebruiker met één authenticatie stap toegang krijgt tot meerdere assets heet “single sign-on”. Op het gebied van ICT is het principe van “single sign-on” breed bekend. Een gebruiker logt éénmaal in, en kan daarna bij allerlei resources op diverse netwerken. Een voorbeeld hiervan is het gebruik van

[7] Gedurende het programma heette dit de “satéprikker”.
[8] Zie voor meer informatie over authenticatie de memo over iris op afstand (Kwaijtaal, Van Munster, Van Rest, Sandbrink, & Van Voorthuijsen, 2015).

de login-procedure van één social media website (bijv. facebook) ook voor andere websites. Een ander voorbeeld is het Kerberos protocol dat gebruikt wordt voor single sign-on van ICT netwerken (MIT, 2015). Kerberos werkt met behulp van virtuele tickets die voor de duur van een sessie worden afgegeven.

In de fysieke wereld heeft een fysiek ticket voor de duur van een bezoek geen toegevoegde waarde. Het zou zelfs extra handelingen vereisen ten opzichte van een permanente badge. Het enige voordeel is dat het ticket buiten het object niet meer geldig is, en dat kwijtraken ervan dus minder een probleem is.

Single sign-on biedt zowel de kans als de verplichting om de overgebleven authenticatieprocedure te verbeteren. Het is een kans, omdat hierdoor het aantal procedures kleiner wordt en er dus meer aandacht kan worden besteed aan de resterende procedure, en de cumulatieve hinder minder kan worden gemaakt. Het is echter ook een verplichting omdat de impact van een persoonsverwisseling groter is geworden: meer assets raken gecompromitteerd als het mis gaat.

7.5 Fysieke single sign-on

Mogelijk kunnen in bepaalde beveiligingsconcepten de twee traditionele authenticatiefactoren “bezit” (bijv. van een pas) en “fysieke karakteristiek” (bijv. middels irisherkenning) voor bepaalde compartimentsovergangen worden vervangen door de twee authenticatiefactoren “tijd” en “plaats”. In andere woorden, is het mogelijk om een persoon met een bepaalde zekerheid te volgen naar een volgend authenticatiemoment, met als doel dat hij daar niet opnieuw hoeft te worden geauthentiseerd? Dat zou effectief betekenen dat het systeem een virtueel ticket aanmaakt bij het begin van een bezoek, dat middels een vorm van tracking wordt gekoppeld aan een individu, en dat op die wijze met hem meereist door alle compartimenten.

In dit programma zijn drie groepen technologieën verkend waarmee mensen gevolgd kunnen worden, echter in ieder geval voor een andere use case:

- In de bouwsteen persoon begeleidingssysteem is verkend in hoeverre draadloze communicatietechnologie geschikt is voor het begeleiden van bezoekers (Van Rest, Sandbrink, & Van Voorthuijsen, Experiment Persoon Begeleidingssysteem (PB), 2015). Dit noemen we coöperatieve tracking omdat de persoon meewerkt door zelf een draadloze tag mee te dragen.
- In de bouwsteen Intelligente Dreigingsdetectie is verkend in hoeverre afwijkend gedrag bij de toegangspoort kan worden gedetecteerd middels video tracking (Van Rest, Voorthuijsen, Sandbrink, Roosjen, & Haeren, 2015). Dit noemen we non-coöperatieve tracking omdat de persoon wordt gevolgd ook als hij niet mee werkt.
- In de bouwsteen Interactieve informatie gestuurde toegangsregulering is verkend in hoeverre iris-op-afstand geschikt is om authenticatie te doen bij toegangsregulering (Kwaijtaal, Van Munster, Van Rest, Sandbrink, & Van Voorthuijsen, 2015). Dit is strikt gezien geen tracking. Echter, indien de lijst met biometrische templates op basis van tijd en plaats wordt beperkt tot diegenen die daar dan kunnen zijn, dan zou het ook in aanmerking kunnen komen. Afhankelijk van de mate waarin de persoon mee moet werken met

het afgeven van biometrie (bijv. het tonen van zijn iris aan een irisscanner), is het een meer of minder coöperatieve variant.

In theorie zouden deze technologieën de benodigde minimale functionaliteit moeten kunnen leveren. Het zal echter ook nodig zijn om alert te zijn op meelopers, waaronder mogelijk zelfs indringers. De coöperatieve vormen van lokalisering zijn daarvoor niet geschikt. Er moet dus minstens ook een niet-coöperatieve vorm van tracking of althans meeloperdetectie worden toegepast.

Ook moet er worden gedacht aan fallback procedures indien de lokalisering niet goed werkt. Mogelijk moet een TBP dan “handmatig” worden gevolgd of moeten er alsnog badges kunnen worden gebruikt bij iedere compartimentsgrens.

7.6 Single sign-on vereist risk-based security

Er zijn in Nederland geen standaarden of zelfs duidelijke generieke good-practices beschreven op basis waarvan kan worden besloten bij welke objecten of welke dreigingen dit –of een ander- principe kan worden toegepast. Dat betekent dat deze keuze dus lokaal moet worden gemaakt en moet worden onderbouwd. Dat vereist dus risk-based security (Van Voorthuijsen, Sandbrink, & Van Rest, 2015).

8 Conclusies en aanbevelingen

Het is nodig en mogelijk gebleken om het complexe concept hinder te operationaliseren. In deze memo is dat gedaan middels de hindermatrix. Deze is een combinatie van drie soorten hinder:

- De mate van detail van informatie
- De gemiddelde vertraging (tijd)
- De mate van verlies van autonomie

Criteria 1 en 3 zijn de mate van invasiviteit zoals beschreven in paragraaf 6.4.1 van (Van Rest, Roelofs, & Van Nunen, Afwijkend Gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid–tweede herziene druk. No. TNO 2014 R10987., 2014).

Deze operationalisering kan gebruikt worden in combinatie met de aanpak zoals beschreven in het rapport over de psychosociale gevolgen van hinder (Nijdam, Olff, Vries, Martens, & Gersons, 2008). Het gebruik van de hindermatrix moet niet in de plaats komen van die aanpak.

Het onderzoeksprogramma waarbinnen deze memo geschreven is, ging over fysieke veiligheid. Echter, de aanpak die in deze memo gehanteerd is, is generiek toepasbaar op ook cyberveiligheid.

8.1 Gebruik van de hindermatrix bij een beveiligingsopdracht

Bij een beveiligingsopdracht kan de hindermatrix gebruikt worden om beveiligden en hun naasten een idee te geven van de te verwachten hinder. Hiervoor is het niet nodig om de eerste kolom met de beveiligingsmaatregelen ook te tonen. Dit is daadwerkelijk middels een drietal gedachte-experimenten beproefd met echte beveiligers (Nieuwenhuijs, Oolbekkink, & Van Rest, 2015). De bevindingen van dat experiment worden hier herhaald:

De twee onderzoekshypotheses waren:

A. Het expliciteren van hinder tijdens de ontwerpfase zorgt er voor dat het resulterende beveiligingsplan minder hinder oplevert.

B. Het expliciteren van hinder tijdens de ontwerpfase zorgt er voor dat de TBP de beveiliging meer accepteert.

De conclusies naar aanleiding van het experiment zijn:

1. Het gebruik van de hindermatrix leidt waarschijnlijk tot beveiligingsplannen die tot minder hinder leiden voor de TBP. In deze casussen zou met name de vertraging door beveiligingsmaatregelen minder worden, en in mindere mate ook de informatie invasiviteit. Hypothese A wordt daarmee voorzichtig bevestigd.
2. Het begrip hinder werd door alle geïnterviewden onderkend als een belangrijke waarde in het samenstellen van een beveiligingsplan.

3. Door alle beveiligers werd (in sterk wisselende mate) uitgesproken dat hiermee in de huidige situatie al voldoende rekening werd gehouden, meestal op basis van ‘onderbuikgevoel’ of in interactie met de beveiligde. Hypothese B wordt daarmee voorzichtig ontkracht. Echter, het lijkt niet te rijmen met de eerste conclusie. Zie voor een beschouwing daarop paragraaf 5.2 Discussie van die memo.
4. Er was geen kritiek op de operationalisatie van hinder zoals in deze memo is gedefinieerd.
5. De toepassing is verkend van het aanpassen van beveiligingsplannen om daarmee minder hinder te creëren. Voor die toepassing werkt de hindermatrix alleen als ze geïntegreerd wordt met een tool waarmee ook snel inzicht in het beveiligingsniveau kan worden gegeven. Alleen op die manier krijgt de gebruiker direct inzicht of de alternatieve beveiligingsmaatregelen (i.e. die met minder hinder) ook voldoen aan de beveiligingsopdracht. In deze studie is daar in een spreadsheet een apart onderzoeksinstrument voor gemaakt.
6. De aanname achter dit experiment is dat er alternatieve beveiligingsmaatregelen ingezet kunnen worden die ook voldoen aan de beveiligingsopdracht (en het weerstandsniveau), maar die minder hinder opleveren. Dit kan alleen indien de beveiligingsopdracht die vrijheid toestaat, en dus niet specifieert welke specifieke maatregelen ingezet moeten worden. Het gebruik van de hindermatrix past dus beter bij risico gebaseerd beveiligen dan bij regel-gebaseerd beveiligen (Van Voorthuijsen, Sandbrink, & Van Rest, 2015).
7. De daadwerkelijke inrichting van een beveiligingsplan dient volgens de deelnemers uiteindelijk door een mens besloten te worden en kan niet voorgeschreven worden door een tool. Wel kan deze hierbij een ondersteunende rol hebben.

8.2 Aanbevelingen

1. De hindermatrix is in deze memo gebruikt om voor een aantal bouwstenen van de experimenteeromgeving te motiveren waarom ze minder hinder zouden kunnen opleveren dan alternatieven. Er is ook een serie gedachte-experimenten uitgevoerd die dat ook voorzichtig onderbouwen. Of dit in de praktijk ook zo door beveiligden en hun naasten ondervonden wordt, is echter niet onderzocht. Hierdoor bestaat er een risico dat de onderzochte concepten in de praktijk niet leiden tot minder hinder. Het wordt dus aanbevolen om het verband tussen beveiligingsmaatregelen en de ervaren hinder ook wetenschappelijk nader te onderzoeken.
2. De hindermatrix is bedoeld als operationalisering van het begrip hinder. Het gebruik er van dient te worden ingepast in de bestaande werkwijze. Paragraaf 5.4 geeft daar een aantal suggesties voor. Het wordt bijvoorbeeld aangeraden om (de theorieën achter) de hindermatrix ook op te nemen in de opleiding van beveiligers. Daardoor kunnen zij zelfstandig beter rekening houden met dit aspect.

3. In diverse bouwstenen van het onderzoeksprogramma zijn verschillende opties verkend om de hinder voor TBP's te verminderen. Het combineren van deelconcepten kan de hinder nog verder verminderen, bijvoorbeeld middels het concept: ”single sign-on”. Het wordt aangeraden dit concept voor fysieke beveiliging verder te verkennen.

9 Referenties

[1] K. De Jong, A. Kwaijtaal, Verkoeijen and I. Weima, "Bewaken en Beveiligen – een basis voor de experimenteeromgeving; rapport TNO-DV 2011 A431," TNO, 2011.

[2] M. Garcia, Design and evaluation of physical protection systems., Butterworth-Heinemann, 2007.

[3] M. J. Nijdam, M. Olff, M. d. Vries, W. Martens and B. Gersons, "Psychosociale effecten van dreiging en beveiliging.," Nationaal Coördinator Terrorismebestrijding, 2008.

[4] R. Van der Kleij, M. Roelofs and D. Van Hemert, "Gaan veiligheidsmaatregelen ten koste van de servicebeleving?," *Tijdschrift voor Veiligheid,* 2015.

[5] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems.," *Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg,* 2001.

[6] D. J. Solove, "A taxonomy of privacy.," *University of Pennsylvania Law Review,* pp. 477-564, 2006.

[7] J. Van Rest, M. Everts, M. Van Rijn and R. Van Paassen, "Het ontwerp van privacy by design," *Privacy & Identiteit,* 2012.

[8] J. Van Rest, M. Roelofs and A. Van Nunen, "Afwijkend Gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid–tweede herziene druk. No. TNO 2014 R10987.," TNO, 2014.

[9] S. Cave, "The free will-scale," Aeon, 19 October 2015. [Online]. Available: https://aeon.co/essays/free-will-is-back-and-maybe-this-time-we-can-measure-it. [Accessed 6 1 2016].

[10] C. Peters and L. De Groen, "Concept of Operations v1.7," TNO, 2015.

[11] A. De Jong and E. Vullings, "The Common Sense Framework," TNO, 2014. [Online]. Available: http://tnopresenter.nl/cs/#/. [Accessed 2016].

[12] R. Hogeweg, S. Van den Brekel, E. Vullings, M.-P. Hasberg and J. Van Rest, "Het nut van een 'natural user interface' voor schaalbaar en effectief interveniëren," TNO, 2015.

[13] R. Van der Kleij, R. Wijn and J. Van Rest, "Prikkelen door bewakers en beveiligers van hoog risico objecten – TNO Memo," 2015.

[14] O. Van der Jagt, M. Jezierska and J. Van Rest, "Beveiligen zonder hinder: detectie van explosieven en wapens," TNO, 2015.

[15] J. Van Rest, R. Sandbrink and G. Van Voorthuijsen, "Experiment Persoon Begeleidingssysteem (PB)," TNO, 2015.

[16] P. Bouthoorn, R. Deckers, C. Haeren, L. d. Groen, G. Van Voorthuijsen, R. Sandbrink and J. Van Rest, "Experiment AV Mobiel," TNO, 2015.

[17] MIT, "Kerberos: The Network Authentication Protocol," 2015. [Online]. Available: http://web.mit.edu/kerberos/. [Accessed June 2015].

[18] J. Van Rest, G. Voorthuijsen, R. Sandbrink, F. Roosjen and C. Haeren, "Experiment Intelligente Dreigingsdetectie: Niet-cooperatieve tracking voor de detectie van afwijkend gedrag," TNO, The Hague, 2015.

[19] A. Kwaijtaal, R. Van Munster, J. Van Rest, R. Sandbrink and G. Van

Voorthuijsen, "Studie Informatiegestuurde Toegangsregulering (IT) – Biometrie on the Move," TNO, 2015.

[20] G. Van Voorthuijsen, R. Sandbrink and J. Van Rest, "Workshop Intelligente Compartimentering (IC) - Risk-based beveiligingstool," TNO, 2015.

[21] A. Nieuwenhuijs, M. Oolbekkink and J. Van Rest, "Beveiligen zonder Hinder: Experiment Hindermatrix," TNO, 2015.

A Mate van invasiviteit

Mate van invasiviteit		Mate waarin persoon autonomie moet inleveren						
		Persoon hoeft niet mee te werken			Persoon moet mee werken			
		Geen	Geïnformeerd	Zichtbaar	Dragend	Vragen om gedrag	Inperken van gedrag	Ter beschikking
Mate van detail van persoonlijke gegevens	Geen	(0) Geen surveillance	Nep surveillance					
	Locatie en uiterlijk	Verborgen surveillance zonder in kennisstelling	(1) Verborgen CCTV camera met in kennisstelling	Menselijke surveillant; CCTV camera		Gezichtsherkenning onder gecontroleerde omstandigheden	(5) Sterke prikkels; In de weg gaan staan	Interview
	Identiteit en locatie		Verborgen CCTV camera met identificatie op basis van gezichtsherkenning; Mobiele telefoon	(2) CCTV camera met identificatie op basis van gezichtsherkenning	(3) Mobiele telefoon; Actieve RFID; GPS transmitter	Identificatie op basis van gezichtsherkenning		
	Reactie op een prikkel			Iedere zichtbare sensor		(4) Middelsterke prkkels; Aanspreken		Ondervraging
	Onder kleding					Mm-wave radar		(6) Fouilleren
	Interne organen en objecten					Röntgen		(7) Intern onderzoek
	Fysiologische parameters, hersenactiviteit				Hartslag en temperatuur sensor op lichaam	Camera met hartslag en/of met infrared temperatuur sensor		(8) Leugendetectie machine; fMRI