Defensie Materieel Organisatie
Ministerie van Defensie

Smart devices bij Defensie

Van reactief naar proactief

Masterthesis Risicomanagement

G.D.S. (Gerton) de Vos

Studentnummer:

Versiedatum: 19-11-2023

JIVC hét IT-bedrijf van Defensie

Defensie Materieel Organisatie
Ministerie van Defensie

Smart devices bij Defensie

Van reactief naar proactief

Masterthesis Risicomanagement

Auteur: G.D.S. (Gerton) de Vos

Studentnummer:

Universiteit Twente

Drienerlolaan 5, 7522 NB Enschede

Ministerie van Defensie

Kromhoutkazerne, Herculeslaan 1, 3584 AB Utrecht

1e Begeleider Dr. J.H. (Jan-Willem) Bullée

2e Begeleider Dr. G.W.J. (Guido) Bruinsma

Versiedatum: 19-11-2023

Voorwoord

Voor u ligt mijn masterthesis die het sluitstuk vormt van de masteropleiding Risicomanagement die ik heb gevolgd aan de faculteit Behavioural Management and Social sciences (BMS) van de Universiteit Twente. De opleiding heeft mij veel nieuwe inzichten gegeven over risicomanagement, hoe wetenschap bedreven wordt maar ook over mijzelf.

Het onderzoek in deze thesis richt zich op de risico's die gepaard gaan bij de introductie van smart devices bij het Ministerie van Defensie. Het onderzoek is ook binnen dit ministerie uitgevoerd, namelijk binnen de afdeling informatiebeveiliging van het IT-bedrijf van Defensie. Het doel is geweest om Defensie in staat te stellen de transitie van reactief naar proactief te kunnen maken. Dit door een instrument te ontwikkelen waarmee medewerkers op voorhand de risico's in te kunnen schatten om verrassingen achteraf te voorkomen.

Het afstuderen en het schrijven van een thesis is naast het hebben van een fulltimebaan zeker geen eenvoudige klus voor mij geweest en heeft langer geduurd dan ik had kunnen hopen. Ik wil daarom mijn manager - tevens interne opdrachtgever - Marieke van Seeters van harte bedanken voor de kans, tijd en gelegenheid die ze heeft gegeven om deze studie te mogen volgen. Daarnaast natuurlijk de respondenten voor hun medewerking en de thesis-begeleiders. In het bijzonder dank voor Jan-Willem Bullée die mij gedurende het project op een prettige manier heeft begeleid.

Ik vind het belangrijk om te vermelden dat ondanks dat er medewerkers van Defensie hebben meegewerkt aan dit onderzoek, hun en mijn uitlatingen persoonlijk zijn en niet per definitie de mening of standpunten van het Ministerie van Defensie verwoorden of vertegenwoordigen.

Tot slot rest mij u veel leesplezier toe te wensen!

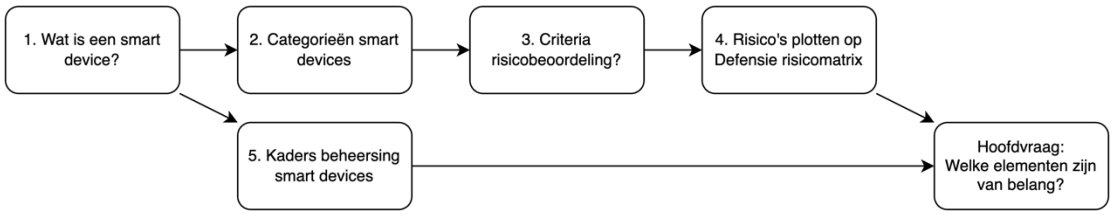
Gerton de Vos
november 2023

Inhoudsopgave

Samenvatting

Defensie is voor nagenoeg al haar activiteiten afhankelijk van producten uit de markt. Naast het voor specifiek militaire doeleinden ontwikkelde materieel - zoals wapensystemen - wordt er ook materieel aangekocht dat niet voor dat specifieke doel is ontwikkeld. Afhankelijk van het gebruik daarvan binnen Defensie wordt dit materieel – wanneer nodig - aangepast voor gebruik voor Defensiedoeleinden. Denk hierbij bijvoorbeeld aan een terreinwagen die in camouflagekleuren wordt gespoten en voorzien wordt van o.a. sterkere vering, stalen bumpers, een wapenrek in de deur en oorlogsverlichting. Technologische ontwikkelingen zorgen ervoor dat veel machines en apparatuur worden voorzien van smart technologie om het leven eenvoudiger en/of veiliger te maken maar binnen Defensie wel voor problemen kunnen zorgen als dit niet (tijdig) onderkend wordt.

Het doel van het onderzoek is het creëren van een model waarmee Defensie in staat zal zijn om de eventuele risico's van aan te schaffen smart devices vooraf in te schatten. Het doel in het onderzoek is het ontwikkelen en valideren van dat model. De afbeelding hieronder laat het conceptuele model van het onderzoek zien.



Figuur 1 - Conceptueel model onderzoek

Hiervoor is het van belang om te leren wat een smart device is en wat er al is geschreven rondom risico-inschatting van smart devices. Welke categorieën smart devices er te onderkennen zijn bij Defensie. Welke criteria van belang zijn voor een goede risicobeoordeling op smart devices. En tot slot op welke manier deze risico's te plotten zijn op de bij Defensie in gebruik zijnde risicomatrix. Voor de beheersing van de risico's is het tevens van belang te onderzoeken of er beveiligingskaders beschikbaar en/of geschikt zijn rondom smart devices.

Het onderzoek is begonnen met de vraag wat een smart device is. Na onderzoek is de volgende definitie gekozen voor een smart device: *"Een smart device is omgevingsbewust, autonoom, kan leren via algoritmes en/of software updates en staat eventueel in verbinding met andere apparaten en/of systemen."*

Onderzocht is welke categorieën smart devices er te onderkennen zijn bij Defensie. Er zijn een 3-tal thema's onderkend. Smart infrastructure, militair materieel en persoonsgebonden devices. Binnen deze thema's zijn sub-thema's met voorbeelden gedefinieerd.

De criteria die van belang zijn om te komen tot een goede risicobeoordeling op smart devices komen neer op beveiligings- en veiligheidsrisico's. Goed is op te merken dat het doel, de kans, van het smart device ook wordt meegenomen in de afweging. De risico's gaan vooral over de beheersbaarheid en de mogelijke consequenties als het fout gaat. Uiteindelijk zijn er een 3-tal criteria van belang om te komen tot een goede risicobeoordeling. Dit zijn Type smart device, context en rubricering.

Voor de beheersing van de risico's is onderzocht welke kaders beschikbaar zijn smart devices. Bestaande kaders voor IT lijken niet goed te passen op smart devices. Uiteindelijk zijn er 3 kaders gevonden die geschikt zijn voor de Europese markt. De IEC 62443, een kader voor de industrie, de ETSI EN 303 645, een kader voor consumentenelektronica en tot slot de ISO/IEC 27400 een kader voor de beveiliging en privacy van IoT.

Voor het plotten risicobeoordelingen voor smart devices op de bij Defensie in gebruik zijnde risicomatrixen is gebruik gemaakt van de gevonden resultaten aangaande categorieën smart devices en de risicocriteria. Vanuit die resultaten is een model ontworpen. Dit model is gevalideerd door de klankbordgroep die samengesteld was met vertegenwoordigers uit de top van Defensie aangaande informatiebeveiliging.

Met de resultaten van de deelvragen samengevoegd is de hoofdvraag beantwoord.
Het hiervoor ontwikkelde model en methode wordt uitgewerkt in een instrument. Defensie moet hiervoor nog de keuze maken met welk(e) kader(s) ze dat willen doen. Het finaliseren van het instrument paste (helaas) niet meer binnen de periode van dit onderzoek en is daarom buiten de scope van deze thesis geplaatst.

Vervolgonderzoek is nodig om te bekijken in hoeverre de markt al klaar is om hun producten te kunnen verantwoorden aan een normenkader. Totdat wetgeving dat afdwingt verdient het de aanbeveling om bij inkooptrajecten kaders te beproeven bij de offerteaanvraag, die te volgen en natuurlijk te evalueren en bij te stellen wanneer dat nodig is.

1 Inleiding

Moderne auto's verzamelen, delen of verkopen je data. Variërend van informatie over hoe hard je rijdt en wat je afspeelt op je radio, tot aan informatie over je seksleven en je medische informatie. Dit allemaal zonder toestemming van de gebruiker (bestuurder) of passagiers zo blijkt uit een onderzoek van de Mozilla Foundation (2023). Tegelijkertijd ziet SonicWall Capture Labs in 2022 een stijging van 87% ten opzichte van 2021 in het aantal Internet of Things (IoT) malware besmettingen naar 112,3 miljoen (SonicWall, 2023a, p. 58). De eerste helft van 2023 laat al een stijging van het aantal besmettingen zien van 37% ten opzichte van 2022. Een aantal van 77,9 miljoen besmettingen wat evenveel is als 2018 en 2019 samen (SonicWall, 2023b, p. 25).

1.1 Ministerie van Defensie

Het Ministerie van Defensie, hierna Defensie, is met ruim 68.000 militairen, burgers en reservisten een van de grootste werkgevers van Nederland (Ministerie van Defensie, 2022). Defensie kent vanuit de Nederlandse grondwet (Rijksoverheid, 1815) een drietal hoofdtaken, dit zijn:

- Het verdedigen van het grondgebied van het Koninkrijk der Nederlanden (inclusief het Caraïbische deel) en dat van haar bondgenoten;
- het beschermen en bevorderen van de internationale rechtsorde en stabiliteit;
- het zowel nationaal als internationaal ondersteunen bij rechtshandhaving, rampenbestrijding en humanitaire hulp.

Voor de uitvoering van deze – bijzondere – taken is de organisatie van Defensie heel divers van aard. Defensie wordt vanwege haar diversiteit aan activiteiten weleens beschreven als 'Nederland in het klein'.

1.2 Probleemcontext

Defensie is voor nagenoeg al haar activiteiten afhankelijk van producten uit de markt. Naast het voor specifiek militaire doeleinden ontwikkelde materieel - zoals wapensystemen - wordt er ook materieel aangekocht dat niet voor dat specifieke doel is ontwikkeld. Afhankelijk van het gebruik daarvan binnen Defensie wordt dit materieel – wanneer nodig - aangepast voor gebruik voor Defensiedoeleinden. Denk hierbij bijvoorbeeld aan een terreinwagen die in camouflagekleuren wordt gespoten en voorzien wordt van bijvoorbeeld sterkere vering, stalen bumpers, een wapenrek in de deur en oorlogsverlichting.

Technologische ontwikkelingen zorgen ervoor dat veel machines en apparatuur worden voorzien van smart technologie om het leven eenvoudiger en/of veiliger te maken maar binnen Defensie wel voor problemen kunnen zorgen als dit niet (tijdig) onderkend wordt. Een voorbeeld hiervan is

dat vrachtwagens tegenwoordig standaard voorzien kunnen zijn van GPS en andere communicatiemiddelen. Dit zodat locatie en wagenstatus doorgegeven kan worden aan het onderhouds- en fleet-managementsysteem. Dat is heel handig in bijna alle situaties, maar als je in een missiegebied met een gecamoufleerde vrachtwagen probeert om niet op te vallen dan helpt het in zo'n geval helpt zeker niet als dit voertuig zich door de communicatie gedraagt als een spreekwoordelijke elektronische kerstboom in een verder donker gebied.

Nieuwe auto's moeten tegenwoordig voorzien zijn van intelligente snelheidsondersteuning waarmee de maximale snelheid van een voertuig situationeel bepaald kan worden (Europees Parlement en de Raad, 2019 (EU)2019/2144, art. 6). Deze functionaliteit is (momenteel) nog wel handmatig uit te schakelen door de chauffeur. Dit vergt wel bewustzijn van deze functionaliteit en dus aanvullende training om te voorkomen dat een door de vijand strategisch geplaatst max. 15km/h bordje langs een route betekent dat een passerend konvooi automatisch gaat afremmen tot 15 km/h.

Naast de ontwikkelingen in de markt is Defensie op zo'n manier georganiseerd dat inkooptrajecten – afhankelijk van het financiële volume dat er mee gemoeid is – op verschillende manieren kunnen verlopen. (Rijksoverheid, z.d.) Van zeer formeel met een (grote) projectorganisatie aan de Defensiezijde vanaf 25 miljoen euro tot aan een incidentele individuele aankoop tot maximaal 2500 euro aan de andere kant van het spectrum. Bij deze laatste variant vindt er behalve het akkoord van de betreffende lijnmanager nauwelijks controle plaats. Het onderzoek zal zich op dit gehele spectrum richten.

Het is om redenen verboden om opnamen te maken op Defensieterreinen (Rijksoverheid, 2022 WvS art. 430). Dit gegeven leidt tot een ander actueel voorbeeld, toevallig ook in de mobiliteitssfeer. Moderne auto's worden door hun zelfrijdende aspecten steeds vaker voorzien van diverse sensoren waaronder camera's (Tesla, z.d.), lidar-sensoren (Volvo, z.d.), e.a. De aanwezigheid van deze sensoren kan leiden tot het onbedoeld lekken van informatie. Zo kan Lidar – onder bepaalde omstandigheden - gebruikt worden om gesprekken af te luisteren (Sami et al., 2020).

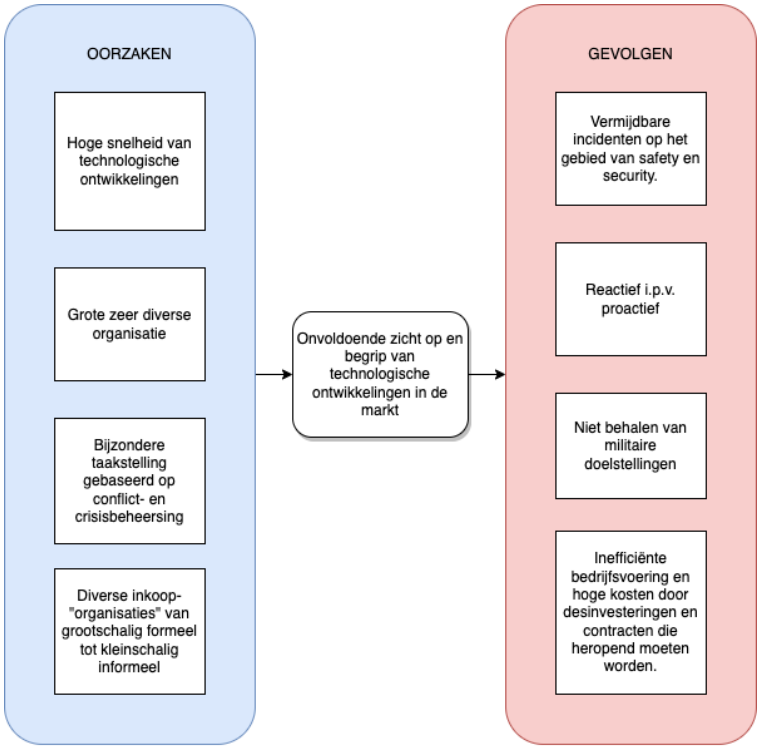
Een laatste hypothetisch voorbeeld zou kunnen zijn dat een militair besluit om een drone te kopen om daarmee mooie beelden te maken van de militaire oefening waar die aan meedoet. De drone zou afkomstig kunnen zijn uit een land met een offensief cyberprogramma (AIVD, z.d.) waardoor er gegevens van die oefening ongewenst bij dat land terecht kunnen komen.

Helaas komt het – door deze snelle ontwikkelingen - regelmatig voor dat de risico's pas achteraf onderkend worden, dus nadat de koop is gesloten en dus van een risico een probleem is geworden. Dat is als de risico's überhaupt al vroegtijdig onderkend kunnen worden omdat sommige mogelijkheden van de technologie pas op een later moment bekend kunnen worden. Dit zijn de zogenaamde "unknown – unknowns" (Taleb, 2016, p. 226).

1.3 Probleemstelling

Technologische ontwikkelingen zoals beschreven in de vorige paragraaf kunnen risico's introduceren en voor problemen zorgen – zowel op het gebied van safety en/of security bij Defensie als ze niet (tijdig) worden onderkend.

Figuur 2 geeft de probleemstelling weer in een oorzaak-gevolgdiagram. In dit diagram wordt weergegeven dat diverse oorzaken zoals de hoge snelheid van de technologische ontwikkelingen, de omvang van de organisatie en de wijze waarop deze georganiseerd is, kan leiden tot diverse gevolgen zoals vermijdbare incidenten op het gebied van safety en security, inefficiëntie, het niet halen van doelstellingen en een grotendeels reactieve wijze van besturen als er onvoldoende zicht en begrip is van de ontwikkelingen in de markt.



Figuur 2 - Oorzaak-gevolg-diagram

1.4 Onderzoeksdoelstelling

Op basis van de probleemstelling kan ook het doel van, en het doel in het onderzoek worden geformuleerd.

1.4.1 Doel van het onderzoek

Het doel van het onderzoek is het creëren van een model waarmee Defensie in staat zal zijn om de eventuele risico's van aan te schaffen middelen vooraf in te schatten. Deze risico's zijn te relateren en te plotten op de risicomatrix zoals die bij Defensie in gebruik is. Hierdoor kunnen passende maatregelen getroffen worden ter bevordering van de (staats)veiligheid en de beschikbaarheid wanneer dat nodig is.

Defensie heeft een bijzondere taakstelling. Zij moet kunnen opereren in het allerhoogste geweldsspectrum en daarbinnen besluiten kunnen nemen over leven en dood. Vanwege deze zeer zware maar ook zeer gevoelige taak zijn sensor-, wapen- en communicatiesystemen buiten de scope van dit onderzoek geplaatst. Het onderzoek zal zich dus primair richten op de vredesbedrijfsvoering van de organisatie.

1.4.2 Doel in het onderzoek

Het doel in het onderzoek is het ontwikkelen en valideren van het model dat hiervoor is beschreven. Hiervoor is het van belang om te leren wat een smart device is en wat er al is geschreven rondom risico-inschatting van smart devices. Welke categorieën smart devices er te onderkennen zijn bij Defensie. Welke criteria van belang zijn voor een goede risicobeoordeling op smart devices. En tot slot op welke manier deze risico's te plotten zijn op de bij Defensie in gebruik zijnde risicomatrix. Voor de beheersing van de risico's is het tevens van belang te onderzoeken of er beveiligingskaders beschikbaar en/of geschikt zijn rondom smart devices.

1.5 Onderzoeksvragen

Om de gestelde doelen van- en in het onderzoek te kunnen behalen moeten een aantal vragen worden beantwoord. Te beginnen natuurlijk met de hoofdvraag.

1.5.1 Hoofdvraag

Welke elementen zijn van belang zodat Defensie de beveiligingsrisico's van smart devices op voorhand kan inschatten en op een passende wijze beheersen?

1.5.2 Deelvragen

Om de hoofdvraag te kunnen beantwoorden is deze opgeknipt in een aantal deelvragen. Als deze beantwoord zijn kan de hoofdvraag worden beantwoord. Deze deelvragen zijn:

1. Wat is een smart device?
2. Welke categorieën smart devices zijn er te onderkennen bij Defensie?
3. Welke criteria zijn van belang voor een goede risicobeoordeling op smart devices?
4. Welke beveiligingskaders zijn geschikt voor de beheersing van de risico's die smart devices met zich meebrengen?
5. Hoe zijn de risicobeoordelingen voor smart devices te plotten op de huidige risicomatrix zoals die binnen het Defensiebeveiligingsbeleid in gebruik is?

In de volgende hoofdstukken zullen de deelvragen worden behandeld en beantwoord. Zodra de deelvragen zijn behandeld kan de hoofdvraag worden behandeld. Het beantwoorden van de hoofdvraag zal gebeuren in het hoofdstuk "Conclusies en aanbevelingen".

1.6 Onderzoeksmethodiek

Om onnodige herhaling te voorkomen worden in deze paragraaf de onderzoeksmethodieken beschreven die meerdere keren bij de beantwoording van de deelvragen gebruikt worden.

1.6.1 Literatuuronderzoek

Niet ieder artikel is even relevant voor de uitvoering van dit onderzoek. Er zijn daarom inclusie- en exclusiecriteria gedefinieerd.
De inclusiecriteria zijn:

- De artikelen zijn gepubliceerd in de Engelse taal;
  Gekozen is voor artikelen in de Engelse taal omdat ik die taal naast het Nederlands het meest beheers.
- Het artikel gaat in op de definitie van smart devices/IoT;
  Het doel van dit onderzoek is inzicht verkrijgen in wat een smart device is. Een artikel dat daar niet specifiek op ingaat draagt daar niets aan bij.
- Het artikel gaat in op de categorieën van smart devices/IoT;
  Het doel van deze vraag is om inzicht te krijgen in de diverse categorieën smart devices. Een artikel dat daar niet specifiek op ingaat draagt daar niet aan bij.
- Het artikel gaat in op de risico's en/of de beheersing van risico's van smart devices;
  Doel van deze thesis is om risico's rondom smart devices in te kunnen schatten en te beheersen. Een artikel dat hierop ingaat wordt dus meegenomen.

- Het artikel gaat in op de kansen van smart devices voor de Defensie-industrie/Defensie-sector.

  Een kans is ook een risico maar dan met een mogelijk positief gevolg. Gekozen is om de scope te beperken tot de Defensie-industrie/-sector om te voorkomen dat artikelen die geen relatie hebben met het beoogde doel worden meegenomen.

De exclusiecriteria zijn:

- Artikelen van voor 2018;

  De ontwikkelingen op het gebied van smart technologie gaat razendsnel. Een 'ouder' artikel verliest daardoor mogelijk sneller zijn relevantie.
- Boekhoofdstukken;

  Boeken zijn lastiger online te verkrijgen. Omwille van de beschikbaarheid zijn boekhoofdstukken van deelname uitgesloten.

1.6.2 Interviewprotocol

De interviewvragen (Bijlage A) zijn opgesteld op basis van de literatuur en de onderzoeksvragen. Daarna zijn 11 experts uitgenodigd om deel te nemen aan de interviews. De experts zijn geselecteerd op basis van hun expertise op het gebied van cybersecurity en/of rol binnen Defensie en zijn zowel werkzaam bij Defensie (9) als daarbuiten (2). De experts zijn werkzaam in de rollen van cybersecurityexpert, wetenschapper, beleidsverantwoordelijke, toezichthouder of lijnverantwoordelijke. De antwoorden van de 2 experts die niet werkzaam zijn bij Defensie worden wel meegenomen bij de beantwoording van de deelvragen. Niet vanwege hun kennis van Defensie maar vanwege van hun kennis van de wereld daarbuiten.

De experts zijn vooraf geïnformeerd over het interviewproces en de vragen die gesteld zouden gaan worden. Het interviewproces is verwoord in het hiervoor opgestelde informed consentformulier. In dit formulier zijn zaken opgenomen aangaande vrijwilligheid, eventuele risico's en over hoe de data wordt verzameld, verwerkt en gebruikt. In dit formulier hebben de geïnterviewden aangegeven hoe zij willen dat er met de naar hun herleidbare persoonsgegevens moet worden omgegaan. Dit formulier hebben ze vervolgens ondertekend en geretourneerd aan de onderzoeker. Afgesproken is dat iedere deelnemer gespeudonimiseerd wordt weergegeven. Gekozen is om de deelnemers een letter toe te kennen en hun rol te veralgemeniseren tot verantwoordelijke, toezichthouder en specialist. Tabel 1 op pagina 14 geeft per geïnterviewde aan of ze bij Defensie werken en geeft hun rol weer.

Verschuren & Doorewaard (2021, p. 211) onderkennen bij interviews/surveys een drietal rollen: Respondent, informant en deskundige. De rol van deskundige past het best bij de kennis, rol en functie van de benaderde personen. Om deze reden is gekozen voor een zogenaamd semigestructureerd interview (Schindler, 2019, p. 130). Deze interviewvorm biedt naast structuur ook de mogelijkheid om hiervan af te wijken en door te vragen en zo meer data en inzichten te verzamelen. Gelet op de expertise van de geïnterviewden is deze vorm van dataverzameling bij uitstek geschikt. De interviews zijn opgenomen en daarna samengevat uitgewerkt (gedeeltelijk getranscribeerd). Eventueel gevoelige zaken zijn hierbij niet opgenomen in de verslagen. De verslagen zijn na uitwerking ter controle en goedkeuring aangeboden aan de geïnterviewden.
Een semigestructureerd interview is een vorm van kwalitatief onderzoek. Om antwoorden toch met elkaar te kunnen vergelijken is gekozen om de antwoorden te coderen. (Boeije, 2009, pp. 96–118) beschrijft 3 stappen van coderen. 1. Open coderen, 2. Axiaal coderen en 3. Selectief coderen. Er zijn op voorhand geen codes gedefinieerd. Het onderzoek is hierdoor inductief van aard. De interviewverslagen zijn gecodeerd op basis van de indeling van de deelvragen volgens de stappen van (Boeije, 2009) waarbij moet worden opgemerkt dat de vragenlijst al een bepaalde selectie (stap 3) afdwingt voor de antwoorden. Voor het coderen is Atlas.ti gebruikt. De UTwente heeft dit softwarepakket aangeschaft ter ondersteuning van kwalitatieve data-analyses.

Onderstaande tabel geeft de geïnterviewden met hun veralgemeniseerde rol weer.

#	Geïnterviewde	Rol	Defensiemedewerker
1	Geïnterviewde A	Toezichthouder	Ja
2	Geïnterviewde B	Toezichthouder	Ja
3	Geïnterviewde C	Specialist	Ja
4	Geïnterviewde D	Specialist	Nee
5	Geïnterviewde E	Specialist	Nee
6	Geïnterviewde F	Verantwoordelijke	Ja
7	Geïnterviewde G	Verantwoordelijke	Ja
8	Geïnterviewde H	Verantwoordelijke	Ja
9	Geïnterviewde I	Toezichthouder	Ja
10	Geïnterviewde J	Toezichthouder	Ja
11	Geïnterviewde K	Specialist	Ja

Tabel 1 – Geïnterviewden

2 Smart devices

Dit hoofdstuk gaat in op de deelvraag: “Wat is een smart device?”
Om deze vraag te kunnen beantwoorden wordt begonnen met wat de wetenschap over dit onderwerp heeft geschreven en welke definitie hiervoor het best te hanteren is. Omdat het antwoord deze vraag meer is dan een paragraaf in een theoretisch kader, verraadt wellicht dat het antwoord op deze vraag nog niet eenvoudig te beantwoorden is.

2.1 Wat is een smart device?

Deze thesis is in het Nederlands geschreven en voor de leesbaarheid wordt de term smart device gebruikt. De Nederlandse vertaling hiervan is echter slim apparaat en met die term is de zoektocht naar duiding van het begrip begonnen.

Een snelle zoekopdracht in het Nederlands naar de term “Slim apparaat” laat met behulp van Google Scholar op de eerste pagina een aantal studies in het Nederlands rondom slimme apparaten zien. Zo stelt Christof Koolen in zijn onderzoek naar de juridische gevolgen van slecht beveiligde Internet of Things (IoT) dat er geen officiële definitie voorhanden is om slimme technologie en IoT te beschrijven maar dat het in veel gevallen over alledaagse apparatuur gaat die is voorzien van sensoren, gegevens verzamelt en die in verbinding staat met het internet (Koolen, 2021, p. 1). Alexander van Deursen gebruikt in zijn rapport over internet- en internet of things-vaardigheden in Nederland anno 2021 de volgende definitie: “Met IoT worden via internet toegankelijke objecten - slimme apparaten - bedoeld die zijn voorzien van detectie-, opslag- en verwerkingsmogelijkheden waarmee deze objecten hun omgeving begrijpen en in staat is om autonoom beslissingen te nemen”. Verder onderkent van Deursen communicatie in het IoT tussen object-object, object-persoon en persoon-persoon. Over deze criteria wijdt hij helaas niet verder uit (van Deursen, 2021, p. 5) (van Deursen & Mossberger, 2018, pp. 124–125).

Opmerkelijk is dat de termen slimme apparatuur (smart devices) en IoT als synoniemen van elkaar gebruikt lijken te worden maar ook dat de auteurs(van Deursen & Mossberger, 2018) & (Koolen, 2021) elkaar tegenspreken op de definitie ervan. Reden dus voor aanvullend onderzoek.

2.2 Methodiek

Omdat er meer in de Engelse taal gepubliceerd is dan in de Nederlandse taal is verder onderzoek gedaan naar de term smart devices om het begrip beter te kunnen duiden. Hiervoor is literatuuronderzoek uitgevoerd. Hierbij zijn de inclusie- en exclusiecriteria gebruikt zoals die in paragraaf 1.6.1 staan beschreven.

Gezocht is met de zoekmachine Scopus.

- Gezocht is in de titel naar Smart Device “TITLE(smart AND device)” N=4732

Vanwege dit aantal resultaten is de zoekopdracht versmalt naar:

- What is a Smart Device “TITLE (what is a AND smart AND device)” N=4

Op basis van de inclusie- en exclusiecriteria zijn de titels en de bijbehorende abstracts gelezen en is uiteindelijk is 1 artikel overgebleven om volledig te lezen. De overige 3 artikelen zijn uiteindelijk afgevallen om de volgende redenen:

- 2 artikelen zijn primair gericht op waarom mensen smart devices kopen.
  Dit aspect draagt niet bij aan doelstellingen van deze studie en voldoet dus niet aan de inclusiecriteria.
- 1 artikel over SHaaS (Smart Home as a Service) viel ook af omdat deze zich primair richt op een commerciële clouddienst van Comcast en daarnaast al uit 2016 stamt wat mogelijk verouderd is. Dit artikel voldoet aan de exclusiecriteria.

Het artikel dat is overgebleven om volledig te lezen is het volgende artikel:
“What is a smart device? A conceptualisation within the paradigm of the internet of things.” (M. Silverio-Fernández et al., 2018). Silverio-Fernández et al. (2018) hebben een systematische review gedaan naar de vraag wat een smart device is. Zij hebben in hun zoektocht de termen “Internet of Things”, “Smart Device” en “Mobile device” gebruikt om tot hun definitie te komen. Zij concluderen op basis van het onderzoek dat de volgende kenmerken typerend en van belang zijn voor smart devices:

Autonomie:	Autonomie gaat over het door het smart device zelfstandig nemen van besluiten zonder dat hier een mens aan te pas komt. Het kan wel zijn dat de mens kaders vooraf heeft meegegeven. Bijvoorbeeld in welke gevallen welk besluit genomen moet worden.
Omgevingsbewust:	Omgevingsbewust gaat over de mogelijkheid van het smart device om metingen te doen over de omgeving waarbinnen het functioneert. Dat gebeurt met sensoren. Hierbij valt te denken aan bewegingssensoren, gps, camera, microfoon, temperatuur-, vochtsensoren, radar, lidar, enzovoorts.
Connectiviteit:	Hiermee is het apparaat in staat om te communiceren met andere apparaten en/of mensen. Dit kan direct tussen apparaten zijn of via een netwerk naar bijvoorbeeld het internet. De technologie en of het netwerkmedium of de omvang van het netwerk maakt in dit geval niet uit.

Zij kwamen in de literatuur ook nog de termen gebruikersinteractie, dataopslag en bij gebrek aan een goed passend Nederlands woord ook mobility/portability tegen. Zij vonden dit echter geen belangrijke kenmerken van een smart device.

Gebruikersinteractie:	Gebruikersinteractie gaat over de communicatie tussen een smart device en de mens. Het apparaat verzamelt en/of geeft data van of aan de mens. Het onderzoek van Silverio-Fernández et al. (2018) beperkt zich tot het paradigma van het Internet of Things. In dit paradigma communiceren apparaten ook vooral met elkaar. Gebruikersinteractie zien zij om die reden niet als een vereiste van een smart device.
Dataopslag:	Een smart device moet zelfstandig kunnen functioneren, dataverzamelen en leren. Silverio-Fernández et al. (2018) ziet dit niet als een separaat kenmerk van een smart device maar vinden dat dit kenmerk opgesloten zit binnen autonomie, omgevingsbewust en connectiviteit.
Mobility:	Mobility ook wel portability wordt ook vaak in studies onderkend blijkt uit het onderzoek van Silverio-Fernández et al. (2018). Vooral in combinatie met de term mobile devices en/of wearables. Zij hebben er echter voor gekozen om dit criterium niet op te nemen in de uiteindelijk definitie om de definitie zo universeel mogelijk toepasbaar te laten zijn.

Uiteindelijk komen Silverio-Fernández et al. (2018) tot de volgende – vertaalde – definitie van een smart device: *“Een smart device is een contextbewust elektronisch apparaat dat autonoom kan rekenen en met andere apparaten bedraad of draadloos verbinding kan maken voor gegevensuitwisseling"* (M. Silverio-Fernández et al., 2018, p. 8).

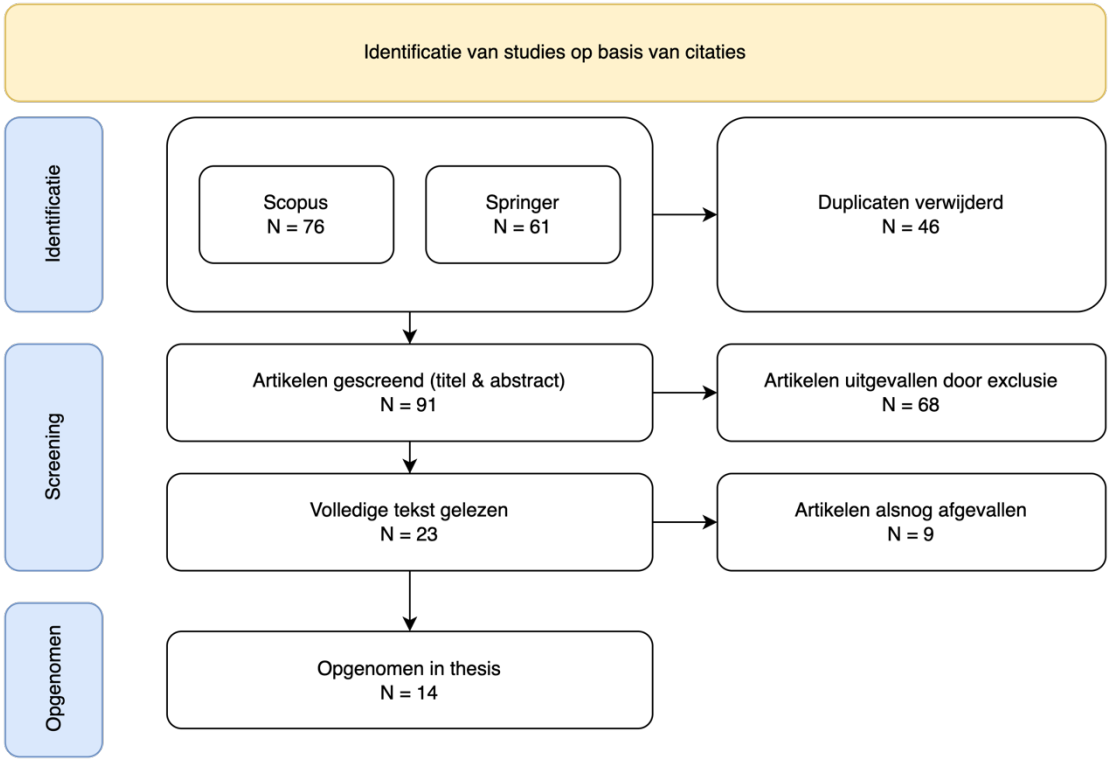
Omdat dit artikel is gepubliceerd in 2018 – wat gezien de snelle technologische ontwikkelingen mogelijk verouderd is – is verder gezocht naar nieuwere of betere definities. Hiervoor is gebruikt gemaakt van aspecten van een systematische review. Gekeken is naar wie dit artikel heeft geciteerd en is gaan voortborduren op het onderzoek dat door Silverio-Fernández et al. in 2018 hebben verricht (M. Silverio-Fernández et al., 2018).

Het artikel van Silverio-Fernández et al. staat zowel op Springer als op Scopus. Op Springer is dit artikel 61 keer geciteerd en op Scopus 76 keer. Door de citaties op deze sites handmatig met elkaar te vergelijken is geconstateerd dat 46 citaties uit beide lijsten overeenkwamen waardoor er 91 artikelen overbleven. Van deze 91 artikelen is de titel en het abstract gelezen. Op basis van de inclusie- en exclusiecriteria zijn hier alsnog 68 artikelen afgevallen waardoor er 23 artikelen overbleven. Deze 23 artikelen zijn volledig gelezen. Uiteindelijk bleek alsnog dat niet ieder artikel voldoende bijdroeg aan dit onderzoek waardoor er alsnog 9 artikelen afvielen. De overgebleven 14 artikelen zijn opgenomen in deze thesis.

De volgende 9 artikelen die zijn afgevallen zijn dat omdat ze niet bijdragen aan de definitie en/of de doelen van deze thesis:

- Khalid & Madi (2020) over het off-loaden van rekenkracht gebaseerd op fuzzy set theory.
- Subramanian & Nagabushanam (2022) gaan in hun paper over de governance of data-product in een multi-layered IoT-systeem primair in op infrastructuur/architectuurvraagstukken en interoperabiliteit.
- Het artikel van Danev et al. (2021) gaat over het ontwerpen van een smart-home omgeving op basis van Open Source software.
- Pallavi et al. (2022) hebben een survey gehouden over de toepassing van IoT binnen industrie 4.0. Hoewel dit artikel wel kort de uitdagingen op het gebied van aanvallen, beveiliging en privacy benoemt gaan ze daar niet verder op in behalve dan dat de respondenten dat ook de belangrijkste uitdaging voor IoT in industrie 4.0 vinden.
- Ndunagu et al. (2022) beschrijven de ontwikkeling van een draadloos sensor netwerk en een op IoT-gebaseerd smart irrigatiesysteem.
- Parhusip et al. (2022) beschrijven in hun paper hoe ze AI en sensoren willen inzetten voor wat ze IntelligenceMining noemen. Dit met als doel om de omgeving te meten om zo milieu- en klimaatverandering te kunnen monitoren.
- Albayaydh & Flechais (2022) gaan naast een herhaling van de aspecten uit Silverio-Fernández et al. (2018) niet verder in op de definitie omdat het onderzoek zich primair richt op een survey rondom privacy concerns onder passanten in Jordanië.
- Het artikel van Schomakers et al. (2022) gaat over hoe privacy een rol speelt in de acceptatie van smart technologieën.
- Vodă et al. (2021) gaan in hun paper in op de kansen van IoT voor het midden- en kleinbedrijf (MKB) op het gebied van innovatie en duurzame groei.

Voornoemde stappen zijn hieronder schematisch weergegeven via een zogenaamd PRISMA-flowchart zoals hieronder afgebeeld in Figuur 3.



Figuur 3 - PRISMA-flowchart

2.3 Resultaten

Fournier et al. (2021) beschrijven een 2-tal "populaire" definities van "Internet of Things" (IoT). Een is volgens hen afkomstig van Van Kranenburg (2008). Dit citaat kan echter niet gevonden worden in het door Fournier et al. (2021) geciteerde werk maar luidt als volgt: *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* (Van Kranenburg, 2008) De andere definitie is afkomstig van Bassi & Horn (2008) en luidt als volgt: *"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"* (Bassi & Horn, 2008).

Volk et al. (2022) hanteren de definitie zoals die door Silverio-Fernández et al. (2018) gehanteerd wordt. Daarnaast geven ze aan dat de apparaten veel data moeten verzamelen om de benodigde diensten te kunnen leveren.

Maestre-Gongora et al. (2020) beschrijven smart technologieën als een combinatie van hardware, software, IT- en communicatietechnologie die samen in staat zijn om data te verzamelen, te analyseren en gedragstrends te voorspellen en daarop qua besluitvorming op aan te passen. De technologieën die daarbij gebruikt kunnen worden zijn onder andere artificial intelligence, big data, ubiquitous computing, databases en sensoren. Zij zien daarnaast een trend met betrekking tot Augmented Reality (AR) en Virtual Reality (VR) in smart technologie.

Silverio-Fernández et al. (2019) beschrijven eigenlijk de definitie die ze in 2018 ook hebben beschreven. Zij baseren zich daarbij vooral op eerder onderzoek gedaan door Miller (2015), Risteska Stojkoska & Trivodaliev (2017) en zichzelf (M. Silverio-Fernández et al., 2018). Hierbij geven ze aan dat eigenlijk alles verbonden kan worden aan het IoT als deze wordt voorzien van de juiste technologie.

Wu & Huang (2020) onderkennen de criteria die door Silverio-Fernández et al. (2018) genoemd zijn met één belangrijk verschil. Autonomie van het apparaat wil niet zeggen dat deze niets anders nodig heeft om te functioneren. In hun onderzoek naar een framework voor off-line operation van smart devices gaan ze ervan uit dat een groot aantal smart devices een internetverbinding nodig heeft om te kunnen functioneren.

Houze et al. (2022) gaan naast de criteria vooral in op het concept explainable AI (XAI). Oftewel kan het apparaat nog aan de mens uitleggen waarom het heeft gedaan wat het heeft gedaan. Ook benoemen zij de term actuator als criterium die smart devices zouden moeten bevatten. Een actuator is nodig om iets in de fysieke wereld te kunnen bedienen. Dan kan variëren van het bedienen van een lamp tot bijvoorbeeld het laten ronddraaien van een wiel.

De Souza et al. (2019) hebben een Rapid Review uitgevoerd naar wat smartness is met betrekking tot IoT. Een Rapid Review is een verkorte versie van een systematisch literatuuronderzoek. In het door hen uitgevoerde onderzoek hebben zij de volgende criteria onderkend:

- Omgevingsinformatie (data acquisitie, -analyse, -transmissie)
- AI (AI-algoritmen)
- Dingen (sensoren en wearables, actuatoren, decision maker)

Opvallend is dat De Souza et al. (2019) onderscheid lijkt te maken tussen het (AI)algoritme en het feitelijke besluit. In hun studie schrijven ze wel dat er duidelijke associaties zijn tussen de 2

begrippen. Uiteindelijk beschrijven ze smartness in dit kader als een IoT-softwaresysteem dat informatie kan verzamelen uit de omgeving en die informatie kan gebruiken om besluiten te nemen en te handelen (De Souza et al., 2019).

Sikder et al. (2021) beschrijven naast de criteria van Silverio-Fernández et al. (2018) ook expliciet self-learning en accessibility als criteria in hun onderzoek naar sensor-gebaseerde dreigingen en aanvallen op smart devices en smart toepassingen.

- Met self-learning bedoelen ze dat het aparaat is staat is om gebruikspatronen te herkennen en zich daarop aan te passen. Als voorbeeld geven zij een smart kamerthermostaat die het gebruikspatroon kan herkennen en de temperatuur daarop kan aanpassen om kosten te besparen.
- Onder accessibility verstaan zij de mogelijkheid om op een eenvoudige manier het apparaat op afstand te kunnen bedienen of te monitoren. Als voorbeeld geven zij een smart slot dat je op afstand eenvoudig met je smartphone kunt bedienen.

Zij (Sikder et al., 2021) vinden wel nadrukkelijk dat rekenkracht een verplicht onderdeel is van een smart device want zonder rekenkracht kan het apparaat niet in staat zijn om de functionaliteiten van een smart device te bieden (autonomie, omgevingsbewust, zelflerend).

K. & M. (2019) gaan in hun onderzoek naar machine learning (ML) technieken vooral in op de hoe vraag rondom op welke manier autonomie ingevuld kan worden. Zij spreken over wireless sensor netwerken als onderdeel van het IoT en onderkennen daarnaast vier basiselementen die elk IoT-gebaseerd ecosysteem zou moeten hebben. Dit zijn apparaat, gateway, Cloud platform en applicaties. Ze moeten daarnaast van nature self-configurable, -manageable, -optimisable, -healable en -adaptive zijn.

Gochoo et al. (2021) beschrijven bij smart devices vooral de definitie van (Silverio-Fernández et al. (2018). Ze noemen daarnaast ook wel artificial intelligence, stem-gebaseerde protocollen en actuatoren.

Llanez-Caballero et al. (2023) beschrijven smartness vooral als apparaten die mensen ontzorgen. Dit in tegenstelling tot hun domme tegenpool waarvoor nog veel interactie en alertheid nodig is. Ze komen ook de term intelligent tegen. Een intelligent product zou in staat moeten zijn om te leren, te anticiperen en onafhankelijk te acteren. Ze (Llanez-Caballero et al.) beschrijven tevens dat er geen goede definitie beschikbaar is en dat de meeste onderzoekers die dit proberen te

doen gebruik maken van subjectieve functionaliteiten en/of technische eigenschappen die lastig te generaliseren zijn. Los van de vage termen zoals intelligentie en complexiteit is het wel duidelijk dat smart devices, digital, connected en responsive zijn.

Cao & Liu (2020) stellen dat de term smart device over het algemeen refereert aan apparaten die kunnen communiceren en rekenen van een simpele sensor tot aan de veelgebruikte smartphone. Later nuanceren ze deze stelling door daar ook aanpasbaarheid en lerend aan toe te voegen. Ze (Cao & Liu) refereren bij de communicatie tussen apparaten wel nadrukkelijk over draadloze protocollen.

(Sepasgozar et al., 2020) beschrijven de term smart als een trend met als doel de verhoging van kwaliteit in de gebouwde omgeving, inclusief huizen, transport, de bouw en stad. Qua definitie hanteren ze verder eigenlijk de definitie van (M. Silverio-Fernández et al., 2018).

Silverio-Fernández et al. (2019) herhalen in deze studie over critische succesfactoren bij de implemantie van smart devices in de bouw hun definitie van hun studie in 2018 (M. Silverio-Fernández et al., 2018). Ook hier herhalen ze dat gebruikersinteractie niet noodzakelijk is maar netwerkconnectiviteit is absoluut noodzakelijk stellen ze. Daarmee volgen ze de definitie die ook door Risteska Stojkoska & Trivodaliev (2017) hiervoor wordt gegeven.

Tabel 2 op de volgende pagina (23) geeft de belangrijkste resultaten per artikel weer. Het bronartikel van Silverio-Fernández et al. (2018) is daarbij gebruikt als startpunt en daarom ook opgenomen in te tabel op regel 1. Daarmee is het uiteindelijke aantal opgenomen artikelen dus 1 artikel hoger dan in Figuur 3 op pagina 19 weergegeven. De tabel borduurt voort – qua codering – op de criteria zoals Silverio-Fernández et al. (2018) die onderkend hebben tijdens het door hen uitgevoerde onderzoek naar de definitie van een smart device. De criteria die zij hebben uitgesloten vanwege hun scopebeperking naar het paradigma van het “Internet of Things” zijn voor de volledigheid wel opgenomen in dit onderzoek. Dit zijn: Connectiviteit, Gebruikersinteractie, Autonomie, Omgevingsbewust, Dataopslag, Mobility. Ook is de gebruikte onderzoeksmethodiek opgenomen in de lijst om de volgende reden. Om te komen tot een goede einddefinitie is het van belang dat de gebruikte onderzoeksmethodiek bekend is. De ene methodiek biedt immers een betrouwbaardere uitkomst dan de andere.

#	Referentie	Onderzoeksmethodiek	Connectiviteit	Gebruikersinteractie	Autonomie	Omgevingsbewust	Dataopslag	Mobility	VR/AR	Lerend	Actuator	Remote access
1	(M. Silverio-Fernández et al., 2018)	S	X	(X)	X	X	(X)	(X)				
2	(Fournier et al., 2021)	L	X	X	X	X		X				
3	(Volk et al., 2022)	E	X		X/AI	X						
4	(Maestre-Gongora et al., 2020)	S	X	X	X/AI	X	X		X	X		
5	(M. Silverio-Fernández et al., 2019)	L	X		X	X			X			
6	(Wu & Huang, 2020)	E	X	X	X	X	X					
7	(Houze et al., 2022)	L	X	X	X/AI	X					X	
8	(De Souza et al., 2019)	S	X	X	X/AI	X	X				X	
9	(Sikder et al., 2021)	S	X	X	X	X	X/A			X		X
10	(K. & M., 2019)	L	X		X	X				X		
11	(Gochoo et al., 2021)	S	X	X	X/AI	X		X		X	X	
12	(Llanez-Caballero et al., 2023)	S	X	X	X	X	X			X		
13	(Cao & Liu, 2020)	L	X		X	X						
14	(Sepasgozar et al., 2020)	S	X	X	X/AI	X				X		
15	(M. Silverio-Fernández et al., 2021)	L	X		X	X	X					

Tabel 2 - Schematisch overzicht resultaten literatuuronderzoek

Legenda:

S = Systematische Review
L = Literatuurstudie
I = Interview
( ) = wel genoemd maar als criterium afgevallen
E = Experiment/Empirisch onderzoek
X = Criterium wordt genoemd in de studie
A = Afgeleid (Inferred)
AI = Artificial Intelligence

2.4 Conclusies

2.4.1 Interpretatie

Op basis van de gevonden resultaten kan worden gestart met de interpretatie ervan zodat de vraag kan worden beantwoord wat een smart device is voor het doel van dit onderzoek. Silverio-Fernández et al. (2018) vonden in hun onderzoek naar de definitie in het paradigma van IoT een 6-tal criteria die genoemd werden in combinatie met smart devices. Uiteindelijk achtten zij er 3 relevant. Te weten: Connectiviteit, Autonomie en omgevingsbewust. Dit onderzoek heeft naast de 6 criteria nog een 4-tal criteria gevonden in de literatuur die genoemd worden in relatie tot smart devices. Dit zijn: VR/AR, lerend, actuator en remote access. Alle criteria worden hierna afzonderlijk beschouwd. Voor de duidelijkheid zijn dit: Connectiviteit, gebruikersinteractie, autonomie, omgevingsbewust, dataopslag, mobility, VR/AR, lerend, actuator en remote access.

- Connectiviteit

  Connectiviteit gaat over de mogelijkheid om te kunnen communiceren met andere apparaten in een netwerk. Bijvoorbeeld een smart stofzuiger die de gebruiker via de app op de telefoon laat weten dat die klaar is met de schoonmaakronde of dat het stofbakje vol zit. Ook kun je denken aan een auto die na een ongeval zelf de hulpdiensten belt (Autoblog.nl, 2020). Alle studies vinden connectiviteit een kenmerk van een smart device. Tegelijkertijd valt op te merken dat al deze studies zich in het paradigma van het Internet of Things bevinden. Zo vinden Houze et al. (2022) device-to-device communicatie zelfs een vereiste. Wu & Huang (2020) beschrijven device-to-device communicatie als een levenskwaliteit verhogende functionaliteit. De connectiviteit speelt zich af via netwerken van elke grootte en vorm en via elk denkbaar protocol en netwerkmedium. Hoewel connectiviteit zeker geen onbelangrijke factor is doe je wel smart zijn tekort als je dit als criterium vereist. Zo kunnen auto's ook smart elementen bevatten zonder dat zij verbonden zijn met andere apparaten (Najjar & Bani Amer, 2016). Denk hierbij bijvoorbeeld aan een auto's die ingrijpen om een ongeval te voorkomen of de auto tussen de lijnen probeert te houden. Die zijn voor die functionaliteiten weliswaar niet connected maar wel smart.
- Gebruikersinteractie

  Gebruikersinteractie gaat over de interactie tussen de gebruiker en het apparaat en omgekeerd. Wie dan de gebruiker is van het apparaat wordt in de literatuur in het midden gelaten. Dit zou de (service)monteur kunnen zijn die het apparaat instelt voor gebruik zoals dit gebeurt bij zonnepanelen en koffieautomaten op kantoren (set and forget). Gebruikersinteractie kan ook het primaire doel zijn van het apparaat zoals dit bijvoorbeeld bij

een smartphone of een smart deurbel het geval is. 10 van de 15 studies beschrijven gebruikersinteractie als eigenschap van een smart device. Miller (2015) beschrijft dat het Internet of Things gaat over apparaten die apparaten met apparaten verbindt en vindt daarom gebruikersinteractie geen eigenschap van een smart device. Dezelfde mening wordt onderschreven door Silverio-Fernández et al.in hun studies over smart devices (2018, 2019, 2021). Hoewel gebruikersinteractie vaak nodig is voor de eerste configuratie van smart devices, geldt voor een aantal smart devices dat er daarna geen interactie meer nodig is. Denk hierbij bijvoorbeeld aan een smart kamerthermostaat die eenmaal ingesteld geen verdere interactie meer nodig heeft/vereist. Ook binnen een smart home is dat allerlei smart apparatuur met elkaar communiceert zonder verdere gebruikersinteractie. Bijvoorbeeld de smart home hub die communiceert met de smart verlichting en de smart raambekleding. Hiermee is gebruikersinteractie geen vereist kenmerk voor een smart device.

- Autonomie

  Autonomie gaat over de zelfstandigheid van het smart device en dus of en in welke mate er gebruikersinteractie benodigd is voor de uitvoering van de functionaliteiten. Autonomie gaat dus ook over besluiten nemen. Over de wijze waarop die besluiten worden genomen, hebben K. & M. (2019) hun onderzoek gebaseerd. Autonomie gaat gepaard met algoritmes. Deze algoritmes en modellen kunnen variëren van een (eenvoudige) beslisboom aan de ene kant van het spectrum tot aan AI, machine learning, deep learning en fuzzy logic aan de andere kant van het spectrum. Over autonomie is veel geschreven en komt als aspect dan ook in alle studies terug. Het betreft eigenlijk het smart deel van het smart device. Smartness gaat vooral gepaard met rekenkracht volgens Llanez-Caballero et al. (2023). Apparaten met weinig rekenkracht zijn over het algemeen minder smart dan apparaten met veel rekenkracht tot hun beschikking. Rekenkracht kan worden uitbesteed aan de cloud om zo (fabrikage)kosten en energie te besparen (Wu & Huang, 2020). Voor gedistribueerde rekenkracht is natuurlijk wel een netwerkverbinding benodigd. Voorbeelden van autonomie zijn een zelfrijdende auto maar ook een smart thermostaat die de woning op de gewenste kamertemperatuur brengt als er mensen in huis zijn op een bepaald tijdstip. Zonder autonomie kun je niet spreken over een smart device.
- Omgevingsbewust

  Omgevingsbewust gaat over dat het smart device wat ‘begrijpt’ van de omgeving waarin die zich bevindt. Omgewvingsbewust gaat gepaard met het hebben van sensoren. Net zoals de mens sensoren (zintuigen) gebruikt om kennis op te doen van de omgeving,

geldt dit ook voor smart devices. Zo zal een smartphone op z'n minst moeten weten waar die is als die nuttig wil zijn voor navigatie en een smart sporthorloge zal - wil die het aantal gezette stappen en het hartritme kunnen bijhouden - ook sensoren moeten bevatten. Alle studies hebben het ook over omgevingsbewustzijn in relatie tot smart devices. Hiervoor kunnen een of meerdere sensoren gebruikt worden. Sikder et al. (2021) hebben in hun studie naar sensor-gebaseerde aanvallen en dreigingen hier veel aandacht aan besteed. Zij onderkennen een 3-tal typen sensoren, namelijk:

- Bewegingssensoren zoals accelerometers en gyroscopen. Deze kunnen bewegingen van het apparaat meten.
- Omgevingssensoren zoals licht, nabijheid, temperatuur, audio, camera, barometer, hartslag en vingerafdruk. Deze sensoren kunnen meten wat ze in de omgeving zien. Vergelijkbaar met de menselijke zintuigen, spraak, smaak, horen, zicht en tast.
- Positiesensoren zoals GPS en magnetisch-veldsensoren. Deze sensoren kunnen gebruikt worden op de locatie van het apparaat op de wereld te bepalen.

Deze sensoren kunnen afzonderlijk of in een combinatie worden gebruikt door het smart device voor het maken van keuzes. Hoe meer sensoren hoe meer het smart device van de omgeving zou kunnen begrijpen. Een apparaat dat niet omgevingsbewust is kan geen smart device zijn.

- Dataopslag

  Dataopslag gaat over het kunnen verwerken van de verzamelde sensorgegevens zodat er besluiten genomen kunnen worden door het smart device. Afhankelijk van het apparaat zal de opslag van data in het vluchtige RAM-geheugen plaatsvinden of op grotere opslagmedia in databases al dan niet gebruikmakend van een cloud-infrastructuur. Dit is helemaal waar wanneer geleerd wordt vanuit historische data om trends te leren herkennen om daarmee een bepaalde voorspelling voor de toekomst te doen. Zonder dataopslag is dat niet mogelijk. Denk hierbij bijvoorbeeld aan de smartphone die voorstelt om een route naar de supermarkt of sportschool te plannen op de momenten dat je dat normaalgesproken doet. Dit is gebaseerd op gedragingen uit het verleden. Dataopslag is ook een criterium dat door een aantal studies (7) wordt onderkend. Silverio-Fernández et al. (2018) stellen dat dataopslag is opgesloten in andere criteria zoals omgevingsbewustzijn, autonomie en connectiviteit. Er zijn geen duidelijke argumenten te noemen die dat tegenspreken.

- Mobility

  Mobility gaat over het kunnen meenemen van het smart device, een zogenaamde wearable. Denk hierbij bijvoorbeeld aan een smartphone of een smartwatch. Mobility is een eigenschap die daarom vooral wordt genoemd in combinatie met de term smart mobile devices. Omdat je hiermee o.a. smart homes, smart industry, smart cities en smart buildings buitensluit is dat geen overtuigend kenmerk van een smart device. Silverio-Fernández et al. (2018) onderschrijven dit eveneens samen met het feit dat dit aspect maar in 2 studies terugkomt.
- VR/AR

  VR/AR staat voor Virtual Reality en Augmented reality. Virtual Reality is een virtuele wereld waarin je je kunt begeven. Met behulp van sensoren kun je je daarbinnen oriënteren en bewegen. Augmented reality voegt virtualiteit toe aan de echte wereld, vaak via de camera, lidar in combinatie met locatieservices. Hiermee zou je bijvoorbeeld informatie over een standbeeld kunnen tonen terwijl je met je smartphone op het standbeeld richt maar je kan het ook gebruiken om te gamen. Denk bijvoorbeeld aan de Pokémon Go app voor de smartphone die in 2016 erg populair was (The New York Times, 2016). VR/AR komt in een 2-tal studies terug. Maestre-Gongora et al. (2020) beschrijven dit fenomeen vooral als trend. Silverio-Fernández et al. (2019) benoemen het ook maar gaan ook niet verder in op waarom dit onderscheidend zou moeten zijn in smart devices. Er zijn geen aanvullende argumenten genoemd waarom AR/VR een separaat kenmerk is van een smart device. AR/VR is een verschijningsvorm van een smart device net zoals een robotstofzuiger dat is.
- Lerend

  Met de term lerend wordt bedoeld dat het apparaat in staat is om gebruikspatronen te herkennen en het gedrag daarop aan te passen. Leren gebeurt vooral op basis van de input van de sensoren maar kan ook afkomstig zijn van andere apparaten/machines. Lerend wordt door een 6-tal studies genoemd als een belangrijk aspect van een smart device. Sikder et al. (2021) benoemen dit als een van de voornaamste kenmerken van een smart device samen met aanpasbaarheid. K. & M. (2019) beschrijven dat het leren op diverse manieren kan plaatvinden. Zij onderkennen supervised-, semi supervised-, unsupervised- en reinforcement learning in hun studie naar machine learning technieken. Hoewel lerende algoritmes vooral worden toegekend aan machine- en deep learning kan dit naar mijn mening ook worden bewerkstelligd met een software-update voor op een

bijvoorbeeld beslisboom gebaseerd apparaat waardoor een smart device vanaf dat moment wat meer kan of iets beter kan. Denk bijvoorbeeld aan een HomePod, een smart speaker van Apple die met een software-update ook in staat werd om de omgevingstemperatuur en de luchtvochtigheid te meten (Apple, 2023, par. Softwareversie 16.3). De benodigde sensoren hiervoor waren natuurlijk al in het apparaat aanwezig. Een device dat niet geüpdatet wordt verliest al snel zijn smartness. Denk hierbij bijvoorbeeld aan TV's en smartphones waarnaar een tijdje steeds minder van gaat werken.

- Actuator

  Een actuator is een onderdeel dat op basis van een signaal iets triggert of omzet in beweging. Die beweging kan zowel lineair als roterend zijn. Actuatoren worden in een 3-tal studies genoemd. Vooral (De Souza et al., 2019) beschrijven dit als een belangrijk kenmerk voor een smart device. Voor (veel) smart devices geldt dat zij een handeling uitvoeren (trigger) in de omgeving. Hierbij zou je kunnen denken aan het aandoen van de verlichting, het uitzetten van de kachel maar ook aan het sturen van een bericht. Dit doen een smart device op basis van verzamelde en verwerkte data uit de sensoren. Een device dat geen actuator heeft zou je niet smart kunnen noemen want dan beperkt de functionaliteit zich tot die van een sensornetwerk dat enkel gegevens verzamelt.

- Remote access

  Remote access gaat over de externe toegang tot het smart device via een netwerkprotocol. Denk hierbij aan toegang tot het apparaat via de app, een webpagina maar ook bijvoorbeeld via Bluetooth als het gaat over het openen van een smart slot. Remote access is in 1 studie genoemd. Sikder et al. (2021) beschrijven remote access als opmerkelijke eigenschap van smart devices in hun studie naar aanvallen en aanvalsoppervlakken op smart devices. Voor remote access is connectiviteit een vereiste. Je zou kunnen beredeneren dat bij Remote access het initiatief voor communicatie extern ligt in plaats van bij het smart device zelf. Remote access is dus een variant van connectiviteit en daarom niet onderscheidend genoeg.

Smartness in een smart device

Smart devices worden op verschillende manieren geduid veelal vanuit het paradigma van het Internet of Things (IoT). Termen die genoemd worden zijn onder andere ambient intelligence, hybrid intelligent systems, AI, smart machine, connected devices, intelligent systems, smart mobile devices, cyber physical systems en tot slot Internet of Things. Hoewel er in de detaillering ongetwijfeld verschillen tussen deze termen te benoemen zijn, zijn die over het algemeen onduidelijk,

niet gestandaardiseerd en subjectief (De Souza et al., 2019; Llanez-Caballero et al., 2023). Llanez-Caballero et al. stellen daarbij ook dat het woord smart als toevoeging op technologie en concepten onduidelijk of subjectief is ten opzichte van hun non-intelligente tegenhanger. Oftewel wat het smart device smart maakt en het non-smart device niet (2023).

2.4.2 Conclusies

Dit hoofdstuk is begonnen met de definities van Van Deursen et al. (2021; 2018), Koolen (2021) en Silverio-Fernández et al. (2018). Voor de volledigheid hier nog even opgesomd.
Van Deursen et al.: *"Met IoT worden via internet toegankelijke objecten – slimme apparaten – bedoeld die zijn voorzien van detectie-, opslag- en verwerkingsmogelijkheden waarmee deze objecten hun omgeving begrijpen en in staat is om autonoom beslissingen te nemen"* (2021). Koolen stelt in zijn onderzoek dat er geen officiële definitie voorhanden is om slimme technologie en IoT te beschrijven maar dat het in veel gevallen over alledaagse apparatuur gaat die is voorzien van sensoren, gegevens verzamelt en die in verbinding staat met het internet (2021). Tot slot geven Silverio-Fernández et al. de volgende definitie voor een smart device: "Een smart device is een contextbewust elektronisch apparaat dat autonoom kan rekenen en met andere apparaten bedraad of draadloos verbinding kan maken voor gegevensuitwisseling" (2018).

In de literatuurstudie zijn in het artikel van Fournier et al. (2021) zijn nog een 2-tal 'populaire' definities naar voren gekomen van Van Kranenburg waarbij opgemerkt moet worden dat deze geciteerde definitie niet gevonden kan worden in het gerefeerde document maar luidt als volgt: *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* (2008). De andere definitie is afkomstig van Bassi & Horn en luidt als volgt: *"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"* (2008).
(Llanez-Caballero et al., 2023) beschrijven (ook) dat er geen definitie is voor smart devices maar dat een aantal auteurs stellen dat een "intelligent" product in staat is om te leren, te anticiperen en is onafhankelijk. Dat doet zij met krachtige AI-software, ratio en zelfstandigheid.
Ze stellen wel dat het duidelijk is dat smart devices digitaal, connected en responsive zijn.

Gelet op deze definities valt het volgende te constateren. De definities van Van Kranenburg (2008) en Bassi & Horn (2008) zijn gegeven de huidige stand van de techniek en de wetenschap wat gedateerd. Ook is onduidelijk hoe de definitie van Van Deursen & Mossberger (van Deursen,

2021; van Deursen & Mossberger, 2018) tot stand is gekomen. De definitie van Silverio-Fernández et al. (2018) is op actuele wetenschap gebaseerd maar beperkt zich tot het paradigma Internet of Things.
Koolen (2021) en Llanez-Caballero (2023) geven allebei aan dat er geen echte definitie is voor een smart device. Dit sluit tevens aan bij mijn eigen observatie en geeft me dus de vrijheid om een eigen definitie te geven.

Llanez-Caballero et al. (2023) en Sepasgozar et al. (2020) geven allemaal aan dat smartness te maken heeft met “ontzorgen” en het verhogen van de kwaliteit van leven. Dat kan bijvoorbeeld zijn op het gebied van comfort, beveiliging, veiligheid en interactie met anderen. Ik wil me hierbij aansluiten.

Dit alles in overweging nemende brengt me dat tot de volgende definitie:
Een smart device is omgevingsbewust, autonoom, kan leren via algoritmes en/of software updates en staat eventueel in verbinding met andere apparaten en/of systemen.

3 Categorieën smart devices bij Defensie

Voor een goede risico-inschatting op smart devices is het van belang om te weten welke categorieën van smart devices er zouden kunnen zijn bij Defensie. Dat is relevant omdat bijvoorbeeld een smart camerasysteem met microfoon een ander inherent (privacy)risico heeft dan bijvoorbeeld smart verlichting. Ook zitten er andere inherente (veiligheids)risico's aan een zelfrijdende auto dan aan een robotstofzuiger.

3.1 Welke categorieën smart devices zijn er te onderkennen?

Voor het antwoord op deze vraag is voortgeborduurd op de literatuur die bestudeerd is in het vorige hoofdstuk.

Sepasgozar et al. (2020) hebben in hun onderzoek een aantal domeinen onderkend waarover in de literatuur over smart technologieën wordt geschreven. Dit zijn de domeinen: Industrie, software/telecommunicatie, gezondheidzorg, onderwijs, energie, transport, bouw, overheid en landbouw. Al deze domeinen komen in meer of mindere mate voor bij Defensie. Wel moet gezegd worden dat landbouw zeldzaam is en vooral voorkomt tijdens vredes- en wederopbouwmissies waarbij Defensie een ondersteunende/opbouwende rol toebedeeld heeft gekregen. Binnen het gezondheidszorgdomein hebben Fournier et al. (2021) hun onderzoek uitgevoerd over 'aging in place'. Zij zien sinds de COVID-19 pandemie een proliferatie van technische oplossingen voor digital health. Hierbij zou je kunnen denken aan wearables, smarthomesystemen, safety- en securitysystemen, social systemen en wellness (sport) systemen. Sikder et al. (2021) beschrijven dat smart devices in elk mogelijk toepassingsdomein kunnen voorkomen. Variërend van persoonlijke gezondheid, smart homes en -cities tot aan grote industriële toepassingen. Coa & Liu beschrijven dat de vormfactor van smart devices continu verandert en alom vertegenwoordigd zijn. Van smartphones tot aan horloges, armbandjes en vesten. Alledaagse voorwerpen kunnen smart worden mits voorzien van smart kenmerken. (Zie definitie vorig hoofdstuk). Zij stellen dat de vormfactor van smart devices tegenwoordig onbeperkt is en steeds mee zal lijken om menselijk gedrag (2020, p. 379). Tot slot stellen Silverio-Fernández et al. (2018) dat onder andere de sectoren transport, smart city, smart domotica, smart health, e-governance, assisted living, e-educatie, retail, logistiek, landbouw, automatisering, fabrikage en procesmanagement van smart technologie profiteren.

De genoemde toepassingsdomeinen geven weliswaar een antwoord op de vraag maar voor het doel van het onderzoek zijn deze te abstract van aard. Reden dus voor aanvullend onderzoek.

3.2 Methodiek

3.2.1 Aanvullend literatuuronderzoek

Voor het aanvullende literatuuronderzoek is gebruikt van de inclusie- en exclusiecriteria zoals beschreven in paragraaf 1.6.1. Gebruik is gemaakt van de zoekmachine “Google Scholar”. Hiermee is in de titel gezocht met behulp van de volgende zoekopdrachten:

- categories smart device “allintitle: categories smart device”, N=0

Omdat smart devices vaak in het paradigma van IoT worden genoemd is de zoekopdracht door het toepassen van synoniemen aangepast naar:

- categories IoT (allintitle: categories IoT), N=7

Op basis van de hiervoor genoemde criteria zijn de titels en de bijbehorende abstracts gelezen en is uiteindelijk zijn 2 artikelen overgebleven om volledig te lezen. De overige 5 artikelen zijn uiteindelijk afgevallen om de volgende redenen:

- 1 artikel is geschreven in de Hongaarse taal;
- 4 artikelen zijn afgevallen omdat ze over andere categorieën gingen dan IoT of Smart devices en daarom niet bijdroegen aan de beantwoording van deze vraag.

De artikelen die over zijn gebleven om volledig te lezen zijn de volgenden:

- “A Study about the Different Categories of IoT in Scientific Publications” (Fischer et al., 2020);
- “What Do Practitioners Discuss about IoT and Industry 4.0 Related Technologies? Characterization and Identification of IoT and Industry 4.0 Categories in Stack Overflow Discussions” (Aly et al., 2021).

Na het lezen van beide artikelen is het artikel van Aly et al. (2021) alsnog afgevallen omdat de onderkende categorieën niet passend waren voor het beantwoorden van deze vraag. Zij onderkenden namelijk de categorieën: network management, software development, platform development, hardware management en system management (Aly et al., 2021, p. 11).

3.2.2 Interviews

Naast bestudering van de literatuur is voor de beantwoording ook gebruik gemaakt van interviews zodat de categorieën van smart devices bij Defensie geduid kunnen worden. Hiervoor is het interviewprotocol gebruikt dat in paragraaf 1.6.2.
Voor de beantwoording van deze deelvraag zijn de volgende 2 vragen aan de geïnterviewden voorgelegd:

2. Heb je ervaring met (de introductie van) smart devices op de werkvloer?
    a. Zo ja, welke apparaten of welk type apparaten ben je tegengekomen?
3. Denk je dat er bij Defensie types smart devices zouden kunnen voorkomen die niet in de burgermaatschappij voorkomen en omgekeerd?

De nummering van de vragen is in lijn met de vragen uit het interview. Vandaar dat er niet bij 1 is begonnen maar bij 2 in dit geval. De ervaringsvraag is gesteld in het kader van validiteit van het onderzoek.

3.3 Resultaten

3.3.1 Literatuur

Fischer et al. (2020) hebben hun onderzoek (systematic review) gericht op de categorisering van IoT. Zij constateren dat IoT een breed veld is waar standaardisatie vooralsnog ontbreekt. Ze onderkennen 3 grote categorieën in hun studie: Consumer, Enterprise en Industry. Ze hebben daarnaast een aantal gebieden per categorie opgesomd. Ze geven niet aan wat ze precies met deze gebieden bedoelen of hoe ze aan die gebieden zijn gekomen. Ze stellen wel dat de genoemde gebieden niet limitatief zijn (2020, p. 26). Voor de duidelijkheid zijn de gebieden aangevuld met voorbeelden van apparaten op basis van de eigen interpretatie van de gebieden.

- Consumer, deze categorie bevat apparaten die bedoeld zijn om gebruikt te worden door consumenten.
    - Smart Home devices, zoals smart tv's, - speakers en robotstofzuigers;
    - Wearables, dit zijn apparaten die je op/aan het lichaam draagt zoals horloges, armbanden en ringen;
    - Connected home automation and alarm systems, zoals video deurbellen, smart deursloten, camera's, gordijnen en verlichting.
- Enterprise, deze categorie bevat niet alleen apparaten die gebruikt worden door bedrijven maar ook apparaten die geïnstalleerd of geconfigureerd (moeten) worden door professionals.
    - Smart city devices, stedelijke smart infrastructuur zoals parkeerbeheer, laadpaal-infrastructuur en afvalstoffenbeheer;
    - Environment sensors (for big buildings or fields), klimaat-, temperatuurbeheer;
    - Medical devices, pacemakers, insulinepompjes, alarmeringssytemen voor fitale functies;
    - Vehicles (transportation), auto's, vrachtwagens, shovels en heftrucks;
    - Sensors for bigger buildings, aanwezigheidsdetectie, brand, -rookdetectie, automatische blusmiddelen;

    - Alarm systems (for business), indringerdetectie, toegangsystemen, camera's, bewegingsdetectoren en detectielussen.
- Industry, deze categorie bevat apparaten die gebruikt worden bij productieprocessen. Bij de onderkende gebieden in deze categorie zijn geen aanvullende voorbeelden genoemd omdat de uitleg in de naamgeving zit opgesloten.
    - Machine sensors;
    - Machine control systems;
    - Industrial sensors;
    - Industrial devices with network connection.

Fischer et al. (2020, p. 26) categoriseren medical devices en transportation devices onder enterprise omdat, hoewel ze gebruikt kunnen worden door consumenten, ze geïnstalleerd moeten worden door een professional. Als future work hebben ze opgeschreven dat ze proberen passende categorieën en aanvullende karakteristieken voor elk IoT device te definiëren (Fischer et al., 2020, p. 28).

3.3.2 Interviews

Alle geïnterviewden hebben ruime ervaring met smart devices en de introductie daarvan op de werkvloer of hebben onderzoek naar smart devices gedaan. Op het tweede deel van de vraag – welke categorieën de geïnterviewden zijn tegengekomen - is op basis van de open codering (Boeije, 2009, pp. 96–108) in de interviewverslagen 33 verschillende typen smart devices gevonden. Na axiaal coderen (Boeije, 2009, pp. 108–115) zijn deze verschillende typen apparaten samengebracht tot 16 categorieën. Tot slot is selectief gecodeerd (Boeije, 2009, pp. 115–118) en zijn de 16 categorieën teruggebracht naar 9 categorieën (sub-thema's). De 9 overgebleven categorieën zijn op hun beurt weer ondergebracht in 3 hoofdcategorieën (thema's), te weten: infrastructuur, militaire doeleinden en persoonsgebonden devices.

Er is bij de totstandkoming van de thema's bewust onderscheid gemaakt tussen de diverse subthema's. Dit omdat er andere risico's te onderkennen zijn bij de behandeling en de beheersing ervan. Dit zal blijken en duidelijk worden in het volgende hoofdstuk. Vanwege de leesbaarheid is de term smart weggelaten, geen smart city dus, maar city. Hieronder volgt een uiteenzetting van de thema's, hun sub-thema's met daarbij enkele voorbeelden van smart devices die daarbinnen onderkend zijn. Achter de voorbeelden zijn de deskundigen genoemd die hierover tijdens de interviews hebben gesproken.

1. Infrastructuur

   Dit thema bevat smart devices die vooral te maken hebben met voornamelijk statische objecten zoals kazernes, gebouwen, terreinen, pijpleidingen en industrie.

   a. City, een kazerneterrein, militaire bases en zelfs oefenterreinen zou je kunnen categoriseren als smart city objecten. Binnen dit sub-thema zou je bijvoorbeeld systemen tegen kunnen komen met betrekking tot energiebeheer, laadpalen, afvalstoffenbeheer, parkeerplekkenbeheer (aantal vrije/bezette parkeerplaatsen) en verkeersstromen beheer (Toezichthouder B,J).
   b. Building, dit sub-thema bevat devices die je in gebouwen kunt aantreffen variërend van bijvoorbeeld een sporthal, loods, kantoorgebouw, hotel en restaurant. Binnen dit sub-thema tref je bijvoorbeeld klimaat- en temperatuurbeheersing, verlichting, brandmeldsystemen en blussystemen aan maar ook appliances zoals koffieautomaten en schoonmaakapparatuur (Toezichthouder B, Specialist D,E, Verantwoordelijke F).
   c. Office, dit sub-thema bevat apparatuur die wordt gebruikt om samen te kunnen werken en/of te vergaderen. Dit sub-thema kenmerkt zich doordat apparaten veelal koppelingen of integraties kennen met het IT-kantoornetwerk. Dit in tegenstelling tot de smart building systemen die dat vanwege kun functionaliteiten niet direct vereisen. Binnen de categorie smart office tref je apparaten aan als smartTV's/ -beamers, Video-teleconferencing (VTC) en smart (white) boards (Specialist C,D, Verantwoordelijke F).
   d. Beveiliging, onder beveiligingssystemen verstaan we systemen die als doel hebben een bijdrage te leveren aan de beveiliging van objecten. Dit is als separaat sub-thema onderkend omdat de devices veelal ingezet kunnen worden in meerdere categorieën zoals op kazernes (smart cities) en gebouwen (buildings). Binnen dit sub-thema kan men de volgende typen smart devices aantreffen: camera's (CCTV), detectiesystemen en toegangssystemen (Toezichthouder A,I,J, Specialist C,K, Verantwoordelijke F).
   e. Industrie, hieronder verstaan we systemen die worden gebruikt bij productieprocessen. Van een machine tot aan een volledig productieproces. Binnen dit subthema kun je sensoren voor machines aantreffen maar ook volledige industry control systemen die totale productieprocessen of industrieprocessen monitoren en beheersen (Toezichthouder B).

2. Militair materieel

   Dit thema bevat smart devices die worden ingezet in het operationele domein van de Krijgsmacht. Dit domein varieert van humanitaire hulp tot en met het grootschalige conflict in het allerhoogste geweldsspectrum.

   a. SeWaCo-systemen (Sensor, Wapen & Communicatie), Sewaco is een belangrijke term die binnen Defensie gebruikt wordt voor de beschrijving van sensor-, wapen- en communicatiesystemen. (Ook wel commandovoeringsystemen genoemd.) Met sensorsystemen worden waarnemingssystemen bedoeld die kunnen variëren van radar- en sonarsystemen tot aan bijvoorbeeld drones met (warmtebeeld)camera's of antenne-arrays om communicatie te onderscheppen. Het belangrijkste verschil met de sensoren in het eerdergenoemde sub-thema beveiliging is de doelstelling deze sensoren, nl. het verwerven van inlichtingen, surveillance, verkenningen en doelopsporing. Ook wel ISTAR[1] genoemd. Wapensystemen ook wel effectors genoemd zijn systemen die een bepaald effect leveren in de strijd. Bij deze systemen kun je denken aan smart munitie, smart weapons maar ook aan verdediging/beschermingsmiddelen zoals bijvoorbeeld een armour protection system. Communicatiesystemen zijn systemen die gebruikt worden voor communicatie. Dat kan menselijke communicatie zijn zoals bij radio's het geval is maar ook communicatiesystemen die machines in staat stellen met elkaar te communiceren. Denk hierbij aan satellietsystemen maar ook aan mesh-netwerken waarbij voertuigen en mensen worden geïnformeerd over de situatie op het gevechtsveld. Ook de communicatie tussen een sensor en een effector valt binnen dit sub-thema. Denk hierbij aan een drone die een raket naar een doel stuurt (Toezichthouder A,B,J,K, Specialist C, Verantwoordelijke F,G,H).
   b. Transport, dit sub-thema bevat logistieke- en transportsystemen en bevat naast voertuigen zoals auto's en vrachtauto's ook heftrucks, shovels en (geklimatiseerde) containers. Ook robotvoertuigen zoals de Milrem THeMIS en transport drones tref je in deze categorie aan (Specialist C,E, Verantwoordelijke F,G).

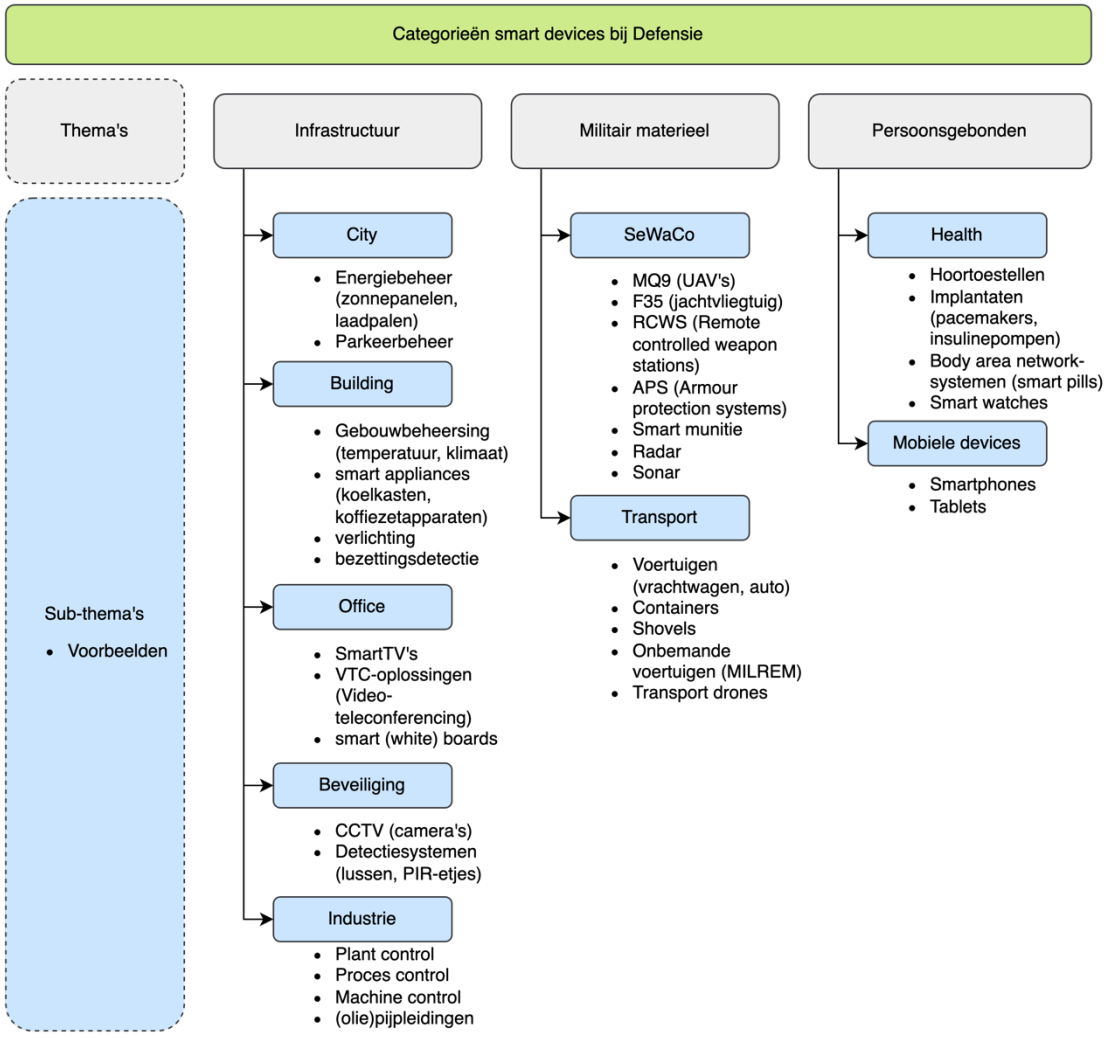
3. Persoonsgebonden

   Dit thema bevat devices die over het algemeen worden toegekend aan - of gedragen worden door - medewerkers van Defensie. Hierbij kun je denken aan de bekende smartphones en tablets maar ook aan smart health devices zoals pacemakers, hoortoestellen, stappentellers en medicijnpompjes.

[1] ISTAR – Intelligence, surveillance, target acquisition and reconnaissance

a. Mobiele devices, dit sub-thema bevat smartphones, tablets en bring-your-own devices zoals laptops. Gelet op het alledaagse karakter van deze apparaten behoeft dit sub-thema geen nadere duiding (Toezichthouder A,B,F,J, Specialist D,K, Verantwoordelijke F).
b. Health, Dit sub-thema bevat medische apparaten zoals bijvoorbeeld een pacemaker, een medicijnpomp of een hoortoestel. Ook vanuit militaire inzet kunnen medische apparaten gebruikt worden om bijvoorbeeld de fysieke gesteldheid van een eenheid in te schatten. Omdat medische gegevens vanuit privacywetgeving als bijzondere persoonsgegevens zijn aangemerkt rechtvaardigt dit een separaat sub-thema (Toezichthouder B,I, Specialist D,K).

Hieronder een schematische weergave van het gevonden model rondom smart devices bij Defensie:



Figuur 4 - Overzicht Categorieën smart devices bij Defensie

3.4 Conclusies

Door het toepassen van de thematische analyse-aanpak (Boeije, 2009) en te coderen in de stappen open, axiaal en selectief was het mogelijk om de genoemde smart devices tijdens de interviews, zoals bijvoorbeeld MQ9-reaper, kamerthermostaat of vrachtwagen te koppelen aan uiteindelijk thema's en sub-thema's. Een risico van selectief coderen is dat je teveel categorieën bij elkaar groepeert waardoor ze mogelijk te algemeen worden om waardevol te zijn. Er is getracht een balans te vinden tussen groeperen en specificeren en recht te doen aan de uitgesproken zorgen van de geïnterviewden tijdens de interviews. Doordat de literatuur in een eerder stadium is bestudeerd, zijn de categorieën uit de interviews te koppelen aan de categorieën zoals die in de literatuur genoemd worden op de specifieke militiaire toepassingen na dan natuurlijk. Het beantwoorden van de deelvraag heeft daarom eigenlijk ook al plaatsgevonden in de vorige paragraaf waar de 3 thema's met daarbinnen de 9 sub-thema's en de gegeven voorbeelden daarbinnen staan benoemd.

Voor de volledigheid staan de thema's en de sub-thema's hieronder nog een keer opgesomd.

1. Infrastructuur
    a. City
    b. Building
    c. Office
    d. Beveiliging
    e. Industrie
2. Militair Materieel
    a. SeWaCo
    b. Transport
3. Persoonsgebonden
    a. Mobiele devices
    b. Health

4 Risicobeoordeling op smart devices

Nu bekend is welke mogelijke categorieën smart devices er te onderkennen zijn bij Defensie, is het nu van belang om te bepalen welke factoren van belang zijn om de risico's ervan te kunnen inschatten. Dit hoofdstuk zal antwoord geven op de vraag: "Welke criteria zijn van belang voor een goede risicobeoordeling op smart devices?" Het antwoord zal zich primair richten op de Defensieorganisatie.

4.1 Welke criteria zijn van belang voor een risicobeoordeling op smart devices?

Martin van Staveren definieert in zijn boek "Risicogestuurd werken" een risico als volgt: "Risico is een onzekere gebeurtenis met oorzaken, een kans van optreden en effecten op doelstellingen" (Staveren, 2015, p. 47). Hij onderkent een 3-tal criteria die samen een risico vormen. Oorzaak, kans en effect op de doelstellingen (impact). Deze criteria worden als handvat gebruikt voor de verdere uitwerking.

Oorzaak

Een risicio kent een of meerdere oorzaken stelt van Staveren (2015, p. 48). De oorzaak is de (on)gewenste gebeurtenis die kan leiden tot een bepaald effect. Uit de eerder bestudeerde literatuur stellen Fournier et al. (2021) dat privacy en beveiliging het belangrijkste zorgpunt is in relatie tot smart (home) technologieën. Ook schrijven ze dat de industrie en de overheid nog grote stappen te zetten hebben rondom privacy van gebruikers en mensen in de omgeving (bystanders) bij het gebruik van wearables. Sikder et al. (2021) hebben onderzoek gedaan naar sensor-based aanvallen op smart devices en applications. Ze stellen dat eerdere onderzoeken naar risico's van smart devices zich vooral hebben gericht op netwerk-gebaseerde aanvallen. Of dat de aanvallen zich richten op de software via kwetsbare frameworks. Daarnaast stellen ze dat onderzoeken rondom beveiliging en privacy van draadloze sensornetwerken zich vooral focussen op dreigingen op communicatieniveau en veelal te generiek beschreven zijn op het gebied van op sensor gebaseerde dreigingen. Sikder et al. (2021) beschrijven 23 verschillende aanvallen op sensoren met verschillende uitwerkingen, van het veranderen van de gps-locatie, dataextractie of hacks via een voor de mens onhoorbaar geluid tot aan het aanpassen van medicatiedoses. Ze vatten deze aanvallen samen in 3 categorieën: kwaadaardige sensor-opdrachten verzenden, onjuiste sensordata injecteren en denial-of-service. Yang et al. (2017) onderkennen 4 categorieën van aanvallen op smart devices binnen het paradigma van IoT. Fysiek/perceptie, netwerk, software en encryp-

tie-aanvallen. Zij scharen de aanvallen op sensoren als fysieke aanvallen omdat je voor een aanval op de sensoren in de buurt van het apparaat moet zijn. Fischer (2022, p. 17) onderkent ook een aantal dreigingen van IoT. Hij beschrijft datadiefstal, letsel aan personen, verminderde veiligheid, denial-of-service, onbetrouwbare informatie, onvoldoende bescherming en onversleutelde data.

Kans

Kansen zijn lastig in te schatten of te bepalen (Staveren, 2015, p. 50). Dit is natuurlijk helemaal het geval als je nog niet weet wat je exact gaat kopen of hoe dat apparaat dan precies ontworpen, gebouwd is en werkt. Historische data kan normaliter helpen bij het inschatten van kansen maar gezien de enorme technologische ontwikkelingen op dit vlak is die - mits voorhanden - nagenoeg onbruikbaar. Een robotstofzuiger van aantal jaren geleden die al flipperend en botsend de ruimte schoonmaakte valt immers bijna niet meer te vergelijken met de huidige versies die op basis van camera's, lidar in combinatie met AI en de cloud totale plattegronden van de omgeving maakt en vakkundig obstakels weet te vermijden. Eventuele dreigingsanalyses – waarbij ook naar kans gekeken wordt – kunnen daarom pas plaatsvinden als er een (voorlopige) selectie van het aan te kopen device heeft plaatsgevonden. Omdat kans wel een belangrijke factor is bij de bepaling van risico's zal de kans van optreden worden bepaald op 100%.

Effect op de doelstellingen

De doelstellingen van Defensie zijn verwoord in de Nederlandse grondwet. Deze staan beschreven in paragraaf 1.1 van deze thesis. De (interne) VIR E&E-risicoanalysemethodiek van Defensie heeft de mogelijke effecten op deze doelstellingen verwoord in een 9-tal potentiële schades voor de organisatie. Defensie noemt dit te beschermen belangen. Afhankelijk van de potentiële omvang van de schade wordt hier een waarde N.V.T., LAAG, MIDDEN of HOOG aan toegekend. De 9 schadescenario's worden langs de pijlers Beschikbaarheid, Integriteit en Vertrouwelijkheid gelegd om te kunnen bepalen waar de risico's voor Defensie en/of de Nederlandse Staat liggen. De 9 schadescenario's zijn:

- Landsverdediging
- Wetshandhaving
- Veiligheid & inlichtingen
- Internationale betrekkingen
- Persoonlijke veiligheid (safety)
- Persoonsgegevens (privacy)

- Verlies aan goodwill (imago/politieke schade)
- Financiële schade (ook juridisch)
- Beleid & werking van processen (bedrijfsvoering)

Afhankelijk van de score van de mogelijke schades komt hier een hoger of lager te beschermen belang uit. Defensie kent 4 categorieën te beschermen belangen (TBB) waarbij TBB-1 het allerhoogste belang is en TBB-4 het laagste te beschermen belang. TBB-2 en TBB-3 liggen daartussen. De risicobereidheid is van de organisatie is gekoppeld aan deze categorieën. Bij deze afhankelijkheidsanalyse wordt de kans van optreden eveneens op 100% gezet.

4.2 Methodiek

Naast bestudering van de literatuur is voor de beantwoording van deze vraag ook het semigestructureerde interview gebruikt. Hiervoor is het interviewprotocol gebruikt zoals dat in paragraaf 1.6.2 beschreven staat.

Voor de beantwoording van deze deelvraag zijn de volgende 4 vragen aan de geïnterviewden voorgelegd:

4. Zie je kansen voor de organisatie door introductie van smart devices?
    a. Zo ja, waarom wel?
    b. Zo nee, waarom niet?
5. Zie je beveiligings-, veiligheidsrisico's voor de organisatie bij de introductie smart devices?
    a. Zo ja, welke zie je?
    b. Zo nee, waarom niet?
6. Welke criteria hanteer je of zou je kunnen/willen hanteren om risico's te kunnen inschatten bij smart devices?
7. Is het type smart device naar jouw mening relevant voor de inschatting van risico's?
    a. Zo ja, gebruik je dan dezelfde criteria (zoals genoemd in de vorige vraag) of komen hier andere criteria bij?
    b. Zo nee, waarom niet?

De nummering van de vragen is in lijn met de vragen uit het interview. Vandaar dat er niet bij 1 is begonnen maar bij 4 in dit geval.

Interviewvragen 4 en 5 zijn gesteld om het probleem bevestigd te krijgen. Immers als er geen kansen (vraag 4) worden gezien voor smart devices dan is de oplossing eenvoudig. Geen smart devices toestaan. Hetzelfde geldt voor vraag 5. Als niemand risico's ziet bij de introductie van

smart devices binnen de organisatie is er ook geen reden of noodzaak om ze te beheersen of er nog langer aandacht aan te besteden.

4.3 Resultaten

Voor de beantwoording van de vragen is de kwalitatieve analysemethodiek toegepast op basis van de grounded theory. Allereerst zijn interviewverslagen open gecodeerd (Boeije, 2009, pp. 96–108), toen axiaal gecodeerd (Boeije, 2009, pp. 108–115) en tot slot selectief gecodeerd (Boeije, 2009, pp. 115–118). Hierbij is rekening gehouden met de doelstelling van dit onderzoek. In de interviewverslagen zijn 76 verschillende coderingen met betrekking tot risico's gevonden. Risico's en risicobeoordelingscriteria zijn hier uiteindelijk opgesplitst.

4.3.1 Kansen

Alle geïnterviewden zien volop kansen voor de inzet van smart devices bij Defensie. Niet alleen op de kazernes in vredestijd maar ook binnen militaire operaties tijdens bijzondere crisissituaties. Mogelijke kansen van smart devices die genoemd werden zijn efficiëntie (kostenbesparingen), vergroten van de effectiviteit en vergroten van veiligheid. Een citaat van een van de geïnterviewden zegt het volgende antwoord op de vraag of er kansen zijn voor smart devices bij Defensie: *"Ja, natuurlijk. Ik denk dat je daarin zoveel als mogelijk gebruik van moet maken. Dit is de werkelijkheid. Als je met een AppleTV beter kunt vergaderen dan moet je die inzetten. Dat moet je natuurlijk wel goed, logisch en veilig inzetten. Daar zit wel de uitdaging. Ik denk dat je nooit belemmerend moet zijn met wat voor techniek dan ook. Wat mij betreft helaas voorbij de ethische grenzen om goed te kunnen begrijpen en leren hoe een tegenstander deze technologie zou kunnen uitbuiten en tegen je gebruiken in het geval van een conflict. Dit om als Defensie je werk te kunnen doen"* (Verantwoordelijke-H).

4.3.2 Risico's

Alle geïnterviewden zien naast kansen ook nadrukkelijk risico's met de introductie van smart devices bij Defensie. Na codering zijn er uiteindelijk 6 risicothema's overgebleven. Te weten: Beveiliging, Veiligheid, Doel, Beheersing, Connectivity en Consequenties. De risico's rondom de thema's beveiliging & veiligheid hebben vooral te maken met doel, beheersbaarheid, consequenties en connectiviteit. Vanuit die gedachtegang is er eigenlijk 1 hoofdthema (beveiliging en veiligheid) te onderkennen met daaronder 4 sub-thema's. Beveiliging gaat om het beschermen van de Defensie-belangen. Dit langs de pijlers beschikbaarheid, integriteit en vertrouwelijkheid. Alle pijlers zijn belangrijk maar vooral dat laatste aspect is erg risicovol voor Defensie. De organisatie heeft immers te maken met (statelijke) actoren die veel kennis en middelen hebben en als doel

hebben om te spioneren, te surveilleren of zelfs te saboteren (Verantwoordelijke-H). Veiligheid is ook een belangrijk thema. Binnen dit thema gaat het niet alleen om de veiligheid van Defensie-personeel maar ook om de veiligheid van mensen daarbuiten. Privacy zit hier als aspect in opgesloten maar ook of het algoritme binnen het smart device wellicht discrimineert of bepaalde vooroordelen heeft richting een groep mensen (Verantwoordelijke-H). Hieronder een schematische weergave van het thema Beveiliging & Veiligheid met de onderkende sub-thema's.

Figuur 5 - Overzicht Risico-thema Beveiliging & Veiligheid

Doel: 4 geïnterviewden hebben doel genoemd als criterium. Als niet duidelijk is met welk doel een smart device wordt gekocht dan zou je het apparaat mogelijk niet moeten kopen. "*Wij stellen altijd de volgende vragen. Waarvoor wil je het gebruiken? Voor welk doel wordt het ingezet? Oefening en/of training? Wat moet het opleveren? Welke risico's heb je zelf al onderkend? De context is dus erg van belang"* (Toezichthouder-J).

Consequenties: Consequenties van besluiten die genomen worden door smart devices werden ook onderkend. Zijn die te overzien en wie is eventueel verantwoordelijk? Een citaat van een geinterviewde ging over het scenario van een zelfrijdende auto en luidt als volgt: *"En wat als het apparaat de mist ingaat? Het is jouw apparaat, jij bent er autonoom mee gaan rijden. En als het ongeval komt omdat je je auto niet tijdig hebt gewassen en er daardoor een sensor vervuild was. Wie is er dan aansprakelijk"* (Toezichthouder-A)?

Beheersing: Binnen het thema beheersing zijn veel risico's onderkend. Binnen dit thema zijn een 4-tal onderwerpen de revue gepasseerd. Veel apparatuur wordt in elkaar gezet met standaardcomponenten en zonder beveiliging in gedachten. De standaardcomponenten kunnen soms meer dan door het apparaat wordt gebruikt. Vaak wordt die extra functionaliteit via software uitgezet maar het is niet gezegd dat het na een eventuele update nog steeds uitstaat. Updates is een ander genoemd risico binnen dit thema. Sommige apparaten krijgen nooit meer een update wat risicovol kan zijn, andere apparaten krijgen feature updates waardoor die meer kan dan eerder was ingeschat en daardoor mogelijk nieuwe risico's introduceert. Controleerbaarheid is ook vaak genoemd in de interviews (19x). Is het gedrag voorspelbaar, wat is het default gedrag van het device bij een storing en hoe kan ik het gedrag testen? Tot slot is dataverzameling en cloudopslag genoemd. Maakt het gebruik van de cloud? Werkt het nog als de cloud er niet is? Van welke cloud wordt er gebruik gemaakt? Welke data wordt er verzonden/opgeslagen/verzameld? Hoe

wordt daarmee omgegaan? Een citaat van een toezichthouder over een smartphone geeft treffend weer hoe complex die vragen soms kunnen zijn. *"Mijn smartphone bijvoorbeeld weet precies waar ik werk, waar ik woon, waar ik vaak kom en welke routes ik gebruik. Terwijl ik dat niet heb ingevoerd of gevraagd aan het apparaat om dat bij te houden. Ik koop zo'n apparaat om bijvoorbeeld mijn e-mail te kunnen lezen en dingen op te zoeken op het internet en ik krijg er een hele waslijst van aanvullende functies bij waarvan de leverancier heeft bedacht dat ik die wellicht zou willen hebben"* (Toezichthouder-A).

Connectivity is het laatste sub-thema. Dit is 21x genoemd in de interviews. Hoewel dit thema een relatie heeft met dataverzameling gaat het verder dan dat. Naast de data-verzameling en eventuele Cloud-verbindingen gaat het ook over integratie binnen bestaande netwerkinfrastructuren zoals dat bijvoorbeeld bij smart-office apparatuur het geval is. *"Elke nieuwe connectie is een nieuwe attack surface"* (Specialist-D). Dat geldt ook voor de sensoren op het smart device. Binnen dit thema zijn ook de netwerkprotocollen, versleuteling, type verbinding genoemd.

4.3.3 Type smart device relevant?

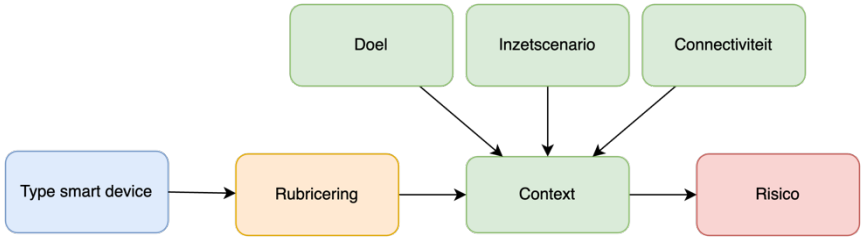
Alle geïnterviewden vinden het type apparaat relevant voor de risicobeoordeling. Een van de geinterviewden had een verfrissende (andere) kijk op de vraag. Deze geïnterviewde stelt dat als je de benefits meeneemt in de risicobepaling het type apparaat niet van belang is. *"Mijn eerste reactie is nee, dat zou – als de context voor de categorieën dezelfde is – niet uit moeten maken. Je zou het kunnen koppelen aan wat wij noemen het inspecteerbare gebied. Een inspecteerbaar gebied is een gebied waarop ik invloed uitoefen. Het wordt wel spannender zodra het apparaat buiten dat gebied komt. Omdat ik de benefits meeneem in de risicobepaling maakt het type apparaat niet uit. Als je deze benefits niet zou meenemen in het eindoordeel, dan is het type apparaat wel van belang"* (Toezichthouder-J). Een ander citaat geeft goed het sentiment weer dat de geïnterviewden hebben aangaande deze vraag. *"Met een slimme thermostaat zal ik uiteindelijk niet heel veel schade kunnen aanrichten behalve dan aan mijn huis en mijn portemonnee. Een slimme auto kan natuurlijk wel veel meer schade aanrichten aan mensen en spullen. Ook het delen van de locatie is natuurlijk risicovoller in bijvoorbeeld een militaire context. Maar ook de componenten die erin zitten"* (Specialist-D).

4.3.4 Criteria risicobeoordeling

Na codering zijn er uiteindelijk 3 criteria overgebleven die van belang zijn voor een risicobeoordeling van smart devices. Dat zijn context, rubricering en type apparaat. Context gaat over de omgeving waarbinnen het smart device moet functioneren en de doelstelling van het smart device.

Dat kan de kazerne zijn, een oefenterrein of een inzetgebied. Daarbinnen is het dreigingsniveau ook van belang waarbij ook de connectivity van belang is. De rubricering – ook wel dataclassificatie – gaat over labeling in relatie tot het beschermen van (Staats)belangen. Binnen Nederland kennen we een 4-tal rubriceringen. Departementaal VERTROUWELIJK, Staatsgeheim CONFIDENTIEEL, Staatsgeheim GEHEIM en Staatsgeheim ZEER GEHEIM (Rijksoverheid, 2013). Tot slot het type apparaat waar in het vorige hoofdstuk aandacht is besteed.

Onderstaande afbeelding geeft de genoemde criteria in een model weer.



Figuur 6 - Criteria van belang voor de risicobeoordeling

4.4 Conclusies

Door het toepassen van de thematische analyse-aanpak (Boeije, 2009) en te coderen in de stappen open, axiaal en selectief was het mogelijk om inzicht te krijgen in de risico's en de risicocriteria die benodigd zijn voor de eerste inschatting van risico's op de introductie van smart devices bij Defensie. Voor het doel van dit onderzoek zijn in eerste instantie 3 risicocriteria van belang om te bepalen of de eventuele aankoop van het beoogde smart device überhaupt wenselijk is om het beoogde smart device te kopen of dat er aanvullend onderzoek nodig is om tot een besluit te komen.

5 Beveiligingskaders

Nu bekend is welke categorieën smart devices er te onderkennen zijn bij Defensie en welke criteria van belang zijn om een risico-inschatting te maken kan worden uitgezocht wat ervoor nodig is om deze risico's waar mogelijk te beheersen.

5.1 Beveiligingskaders voor smart devices

Uit de eerder bestudeerde literatuur onderkennen Volk et al. (2022) geen security frameworks voor smart devices maar wel een aantal privacy-labels voor smart devices. Zoals die uit het Verenigd Koninkrijk, verwoord in de Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security" consultation (Great Britain. Department for Digital, 2020). Het Verenigd Koninkrijk heeft in dit label gebaseerd op de 3 belangrijkste richtlijnen uit de ETSI Technical Specification (TS) 103 645 (ETSI, 2020) aangaande wachtwoorden, contactpersonen en updates. Daarnaast beschrijven ze een Singaporees label (Cybersecurity Certification Centre, z.d.). Bestudering van dat label laat dat deze een 4-tal cybersecuritylevels onderkent. Tier-1 Security Baseline Requirements en Tier-2 Lifecycle Requirements van dit label maken gebruik van de Europese Standaard ETSI EN 303 645 en mogen op basis van verklaringen van conformity worden gevoerd. Level 3 & 4 van dat label zijn alleen te behalen door externe – onafhankelijke – validatie en pentests (CSA Singapore, z.d.). Sikder et al. (2021) beschrijven in hun studie naar sensor-based aanvallen op smart devices wel oplossingen. De door hun beschreven mitigerende maatregelen voor deze aanvallen bevatten geen generieke frameworks maar beschrijven vooral merk specifieke (punt)oplossingen voor een specifiek probleem in de beveiliging. Bijvoorbeeld een IDS-oplossing (Intrusion Detection System) voor een smartphone/smart watch. Sebastian Fischer heeft in zijn dissertatie over "Internet of Things: A Model for Cybersecurity Standards and the Categorisation of Devices" (2022) nadrukkelijk aandacht besteed aan cybersecurity beheersingsstandaarden.

Hij onderkent de Duitse standaard DIN SPEC 27072, de Europese Standaard ETSI EN 303 645, de Radio Equipment Directive, The Common Criteria for Information Technology Security Evaluation, de EU Cybersecurity Act, de General Data Protection Regulation (GDPR) oftewel de AVG, de NISTIR 8259 van het National Institute of Standards and Technology (NIST), het eerder genoemde Britse label dat gebaseerd is op een concept van de ETSI EN 303 645, de ETSI TS 103 645 en tot slot het Finse Cybersecurity Label dat eveneens is gebaseerd op de Europese Standaard ETSI EN 303 645. Op te merken valt dat al deze kaders zich richten op consumenten IoT. Voor industrie en enterprise apparaten is de IEC 62443 (Industrial communication networks - IT security for networks and systems) beschikbaar. Het verschil tussen de IEC62443 en de ETSI

303 645 zit hem vooral in de hoeveelheid beheersmaatregelen en de diepgang/detaillering van de gestelde eisen. Hierbij valt op te merken dat voor consumenten IoT 68 beheersmaatregelen staan genoemd ten opzichte van de 263 beheersmaatregelen voor bedrijven en industrie (Fischer, 2022, pp. 25–36). Naast de bestudering van de literatuur is ook gezocht op NEN-connect naar eventuele andere standaarden aangaande de beheersing van IoT-risico's. Daar is de NEN-ISO/IEC 27400 - Cybersecurity - IoT security and privacy Guidelines gevonden. Dit kader beschrijft beveiligings- en privacy beheersmaatregelen voor zowel de IoT service developer, de IoT service provider als de IoT user.

5.2 Methodiek

Naast bestudering van de literatuur is voor de beantwoording van deze vraag ook het semigestructureerde interview gebruikt. In paragraaf 1.6.2 staat het interviewprotocol hiervoor beschreven.

Voor de beantwoording van deze deelvraag zijn de volgende 2 vragen aan de geïnterviewden voorgelegd:

8. Zijn er – naar jouw weten – (tactische) normenkaders die bestuurders in staat stellen om risico's rondom smart devices (beleidsmatig) te beheersen?
    a. Zo ja, welke ken je?
9. Zijn er – naar jouw weten – voor "medewerkers" hulp-kaders beschikbaar om op een "Safe for Work"-apparaat te kopen?
    a. Zo ja, welke ken je?
    b. Hoe kan een "medewerker" dat herkennen?

De nummering van de vragen is in lijn met de vragen uit het interview. Vandaar dat er niet bij 1 is begonnen maar bij 8 in dit geval.

Deze interviewvragen zijn gesteld om inzicht te krijgen in de beheersingsmogelijkheden van de risico's die met smart devices gepaard kunnen gaan. Om deze risico's inzichtelijk te krijgen en ze passend te kunnen beheersen is het van belang dat de organisatie eisen gaat stellen aan het product en de omgeving waarbinnen die moet functioneren. Kaders en labels kunnen hierbij ondersteunen.

5.3 Resultaten

Voor de beantwoording van de vragen is de kwalitatieve analysemethodiek toegepast op basis van de grounded theory. Allereerst zijn interviewverslagen open gecodeerd (Boeije, 2009, pp. 96–108), toen axiaal gecodeerd (Boeije, 2009, pp. 108–115) en tot slot selectief gecodeerd (Boeije, 2009, pp. 115–118). Hierbij is rekening gehouden met de doelstelling van dit onderzoek. In de interviewverslagen zijn 28 verschillende coderingen met betrekking tot kaders en labels gevonden. Deze coderingen zijn uiteindelijk samengebracht tot een 3-tal thema's. Normenkaders, labels en beheersmaatregelen.

5.3.1 Normenkaders

Met een normenkader wordt een richtinggevende set aan normen bedoeld die toetsbaar zijn door een auditor. Een normenkader kan vanuit een wetgever of beroepsgroep worden opgelegd maar ook binnen een sector worden omarmd als best practice. Binnen het thema normenkaders zijn een 3-tal subthema's onderkend. Bestaande kaders, Dit zijn kaders die nu al gebruikt worden binnen Defensie. Daarnaast bekende kaders, dit zijn kaders die door de geïnterviewden zijn genoemd om de risico's rondom smart devices te beheersen. Tot slot de mogelijke kaders bij instanties. Deze zijn vanuit het meedenken van de geïnterviewden geopperd om verder te onderzoeken.

Bestaande kaders binnen de Defensieorganisatie zoals de Baseline Informatiebeveiliging Overheid (BIO)(Centrum voor Informatiebeveiliging & Privacy, 2023) en het Defensie Beveiligingsbeleid (DBB) zijn genoemd. Ook de Algemene Beveiligingseisen Defensieopdrachten (ABDO) (Ministerie van Defensie, 2019) een kader waaraan bedrijven moeten voldoen als ze een vertrouwelijke opdracht voor Defensie willen uitvoeren. Een citaat uit de interviews hierover: *"Het huidige kader zoals de BIO is denk ik niet dekkend voor smart devices. Veel leveranciers zijn nog niet gewend om met een beveiligingsbril op naar hun apparaten te kijken"* (Toezichthouder-A).

Bekende kaders. Er zijn ook kaders genoemd tijdens de interviews zoals de Radio Equipment Directive (European Commission, 2014) die zich richt op de bescherming van draadloze communicatie zoals bijvoorbeeld het ongewenst mee kunnen kijken of luisteren bij een babyfoon. Ook is een Amerikaans kader voor mobiele devices genoemd, de NIST SP 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise (Howell et al., 2023). Kaders voor de beheersing van industrie-automatisering (ICS-SCADA) werden ook voorgesteld om te overwegen (Verantwoordelijke-G).

Mogelijke kaders. Van de 11 geïnterviewden kenden 8 experts geen specifieke normenkaders voor de beheersing van smart devices maar geven wel suggesties welke instanties mogelijk

daarin zouden kunnen voorzien. Daarbij werden het National Institute of Standards and Technology (NIST) Verantwoordelijke-H, Specialist-K), het Nationaal Cyber Security Centrum (NCSC) (Verantwoordelijk G) en de Rijksdienst Digitale Infrastructuur (RDI) (Specialist-E) getipt. Aan deze tips is opvolging gegeven.
De NIST heeft inderdaad een framework for IoT Device Manufacturers gepubliceerd, de eerdergenoemde NISTIR 8259 (Fagan et al., 2020). Bij het NCSC is eveneens een factsheet aangetroffen genaamd “Basis-beveiligingsmaatregelen slimme apparaten (IoT)” (NCSC, 2023). Dit kader geeft enkele tips rondom het configureren van het netwerk en het smart device. Tot slot is bij de Rijksinspectie Digitale Infrastructuur (RDI) gekeken naar een kader. Daar is geen kader aangetroffen maar wel “tips voor beveiliging van slimme apparaten” (Rijksinspectie Digitale Infrastructuur (RDI), z.d.).

De experts uit de interviews hebben goede inzichten gegeven over de problematiek met kaders. Zo stelt Toezichthouder-A: *“Het lastige met dit soort dingen is dat kaders zich parallel (red. sequentieel?) ontwikkelen aan de technologie. Bijvoorbeeld met het gebruik van algoritmes. Die worden ontwikkeld en daarna denkt men pas na over impact, beveiliging, ongewenste effecten, controleerbaarheid, enz. Er begint zich daarna een normenkader omheen te vormen om het hanteerbaar te maken. Helemaal aan de edge van de innovatie omdat daar nog onvoldoende ervaring is om daar wat van te vinden.”* Toezichthouder-B stelt: *“Het DBB heeft ook iets statisch terwijl de wereld om ons heen erg dynamisch is.”* Specialist E: *”De wetgeving loop hierbij ook jaren achter. Het voormalige Agentschap Telecom, tegenwoordig Rijksinspectie Digitale Infrastructuur hebben richtlijnen opgesteld. Vanuit de EU komen er richtlijnen naar de Nederlandse overheid.”* Welke richtlijnen dat zijn zegt Specialist-D. Die stelt dat de Cyber Resillience Act eraan komt. Hierover in de volgende paragraaf meer.

5.3.2 Labels

Geen van de respondenten is op de hoogte van het bestaan van labels voor smart devices. Wel wisten er een paar te benoemen dat er initiatieven zijn om dat te ontwikkelen. Hierna een 3-tal citaten hieromtrent uit de interviews. *“De CRA komt eraan. De Cyber Resillience Act vanuit de EU en die reguleert “Cybersecurity rules to ensure more secure hardware and software products” een element dat daarin zit is dat er tenminste 5 jaar (security) updates zullen zijn maar ook andere aspecten zoals een level playing field. Maar ook dat is ook een set aan minimum eisen. Maar die is ook niet Safe-for-work want vooral gericht op consumenten, private use. Er komt dus met CRA dus wel wat aan. Europa is zich op dat vlak wel aan het roeren. Maar data-exportaspecten/ risico’s voor naar buiten de EU zitten daar bijvoorbeeld nog niet in.”* (Specialist-D)

"Er zijn wel ideeën voor geweest, een IoT-label. Maar dan zit je ook wel met de discussie van hoe gaan we het doen? Hoe gaan we testen? Wat zit er in zo'n label? Waar ga je op testen? Als al die onderdelen goed zijn, heb je dan ook een veilig apparaat? Dat is volgens mij tot nu toe nog in de discussies gebleven maar er zijn dus wel veel discussies over, onder andere bij en binnen het Agentschap Telecom." (Specialist-E)

"Ik weet dat het Agentschap Telecom en de EU daarmee bezig zijn maar het is er nog niet voor zover ik weet." (Verantwoordelijke H)

5.3.3 Beheersmaatregelen

Vanuit de interviews hebben de experts ook meegedacht over zaken die belangrijk zijn om mee te nemen in de beheersing van smart devices. Genoemd zijn de zaken die zijn opgevallen en zeker kunnen helpen bij de acquisitie van bepaalde categorieën smart devices.

- Algemene aansluitvoorwaarden meesturen in de offerteaanvraag (Toezichthouder-B);
- HBoM (Hardware Bill of Materials) uitvragen bij de offerteaanvraag (Specialist-D);
- Hardeningsinstructies voor het device uitvragen bij de offerteaanvraag (Toezichthouder-B, Specialist-D).

5.4 Conclusies

5.4.1 Interpretatie

Vanuit de literatuurstudie en de interviews zijn een aantal kaders onderkend die kunnen helpen bij de beheersing van de risico's die met de introductie van smart devices gepaard gaan.

Kaders

- DIN SPEC 27072 - Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit, Deze standaard kon niet worden gevonden. Niet in het Engels en niet in het Duits. (Fischer, 2022, p. 27) stelt dat de scope zich beperkt tot smart devices met een IP-verbinding en dat de ETSI EN 303 645 volledieger is en een ruimere scope kent. Het kader richt zich primair op consumentenapparatuur.
- ETSI EN 303 645 is een Europees kader en richt zich op consumenten apparatuur.
- Radio Equipment Directive (RED) is een normatief kader dat geldt voor alle draadloze communicatie tussen devices.
- The Common Criteria for Information Technology Security Evaluation is een wereldwijze standaard die ook verwoord is in de ISO/IEC 15408. Dit is een vrijwillig label en redelijk uitgebreid met 3 delen om gecertificeerd te raken. Het wordt vooral gebruikt als beveiligingseis. Voldoen

aan deze eis is langdurig en complex en daarom minder geschikt voor eenvoudigere apparatuur.

- IEC 62443 – Security of Industrial Automation and Control Systems is een uitgebreid framework dat wordt gebruikt in de industriesector maar inmiddels ook wordt toegepast in de bouw, medische apparatuur en de transportsector (ISA Global Security Alliance, 2023).
- ISO 27400 - Cybersecurity - IoT security and privacy – Guidelines is een norm uit de ISO 27000-serie. Hiermee kan die goed samenvallen met de reeds bestaande kaders zoals de BIO en de voor de zorg verplichte NEN7510. Uit het document wordt de doelgroep niet helder. (Fischer, 2022, p. 77) stelt dat deze standaard zowel geschikt is voor consumenten IoT, Industrial IoT als Enterprise IoT.
- NIST800-124r2 - Guidelines for Managing the Security of Mobile Devices in the Enterprise gaat over het beveiligen van Mobiele devices. De NIST is een Amerikaanse standaard en daardoor wellicht wat minder geschikt voor de Europese markt.
- NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers is eveneens een kader van de NIST. Dit kader is bedoeld voor fabrikanten en onderkent een 6-tal activiteiten waarbij de fabrikant zich moet inleven in het mogelijke gebruik van het apparaat bij de gebruikers.
- NCSC – Basis-beveiligingsmaatregelen slimme apparaten. Dit kader is beperkt van omvang en lijkt niet gericht op grote bedrijven.
- RDI – Tips voor beveiliging slimme apparaten bevat een beperkt aantal tips voor aankopen. Lees reviews en andere praktische tips. Onduidelijk is hoe hiermee de beveiligingswaarde meetbaar kan worden verbeterd.

5.4.2 Conclusies

Er komen kaders aan die het op Europees niveau gaan verplichten (Rijksoverheid, 2023) maar vooralsnog zijn die er niet. Op papier lijkt de ISO 27400 het meest ideale kader omdat het alle domeinen afdekt. Dit kader is redelijk nieuw dus de kans groot is dat leveranciers daar nog niet op zijn ingespeeld. Om te voorkomen dat de markt overvraagd wordt is het verstandiger om aan te sluiten bij kaders die al wat meer tractie hebben binnen de sectoren. Daarbij geldt de IEC 62443 voor de industrie, gebouwenbeheer, de medische sector en het transport, en de EN 303 645 voor de smart appliances. Deze kaders kunnen – indien de context of de rubricering dit vereist – worden aangevuld met Defensie-specifieke beveiligingskaders uit het DBB.

6 Risicomatrix Defensie

Dit hoofdstuk geeft antwoord op de deelvraag over hoe de risicobeoordelingen op smart devices te plotten zijn op de risicomatrix zoals die binnen het Defensiebeveiligingsbeleid in gebruik is?

6.1 Theorie

Voor de beantwoording van deze deelvraag is geen wetenschappelijke literatuur geraadpleegd maar is gebruik gemaakt van interne (beleids)documenten van het Ministerie van Defensie.

6.2 Methodiek

Voor de beantwoording van de deelvraag is gebruik gemaakt van deskresearch ook wel bureauonderzoek genoemd (Verschuren & Doorewaard, 2021, p. 197). Hierbij zijn de volgende stappen uitgevoerd:

Documentenonderzoek

1. In deze stap zijn de beleidsdocumenten binnen Defensie rondom risicomanagement binnen de beveiligingsketen bestudeerd.
2. Vervolgens zijn de onderkende thema's en sub-thema's uit Hoofdstuk 3 geplot op de risicomatrix.
3. Tot slot zijn de risicocriteria uit Hoofdstuk 4 gekoppeld en verwerkt in een model per thema.

Klankbordgroep

Voor de validatie van de resultaten uit het bureauonderzoek zijn deze op 6 oktober 2023 in een sessie van 2 uur voorgelegd aan de klankbordgroep. Deze klankbordgroep is samengesteld uit beleidsverantwoordelijken uit de top van de Defensieorganisatie. Aangesloten waren onder andere de Beveiligingsautoriteit van Defensie (opsteller van het Beveiligingsbeleid en toezichthouder), de Chief Information Security Officer (CISO) van Defensie, verantwoordelijk voor de inrichting van informatiebeveiliging binnen de Krijgsmacht en een Beveiligingscoördinator van de Koninklijke Landmacht, het grootste krijgsmachtsdeel van de Krijgsmacht die dagelijks toezicht houdt op de beveiliging van de diverse informatie- en wapensystemen van de organisatie.

Aan de klankbordgroep zijn de resultaten van het onderzoek en de resultaten van het bureauonderzoek gepresenteerd met de aannames die daarbij zijn gedaan. De klankbordgroep is daarbij uitgedaagd een kritische houding aan te nemen om een zo goed mogelijk eindproduct te kunnen realiseren.

6.3 Resultaten

Resultaten van Stap 1, documentenonderzoek

Vanuit het documentenonderzoek zijn de volgende documenten gevonden op het publicatieportaal (intranet) van Defensie.

- Secretaris-Generaal (SG), SG/003 – Defensie Beveiligingsbeleid (DBB) (10 december 2015)
- Beveiligingsautoriteit (BA), A/005 – Te Beschermen Belangen (1 maart 2020) *
- Beveiligingsautoriteit (BA), A/006 – Risicomanagement (3 december 2018)
- Beveiligingsautoriteit (BA), D/101 – Betrouwbaarheid van informatiesystemen (14 mei 2018)
- Template Statement of Compliance (10-2022)

* De A/005 is VERTROUWELIJK en is op een afgeschermd deel op het netwerk aangetroffen.

Vanuit de SG/003 is bepaald dat de Beveiligingsautoriteit van Defensie verantwoordelijk is voor het ontwikkelen, beheren en evalueren van het DBB. Daarnaast is zij verantwoordelijk voor het toezicht op de naleving van de beveiligingsbepalingen. (p.10)

De A/005 - Te Beschermen Belangen: Vanwege de gevoeligheid van de informatie in dit document is de inhoud zoveel mogelijk veralgemeniseerd in deze thesis. De A/005 onderkent Te Beschermen Belangen (TBB). Dit document verstaat onder een TBB: “Materieel en informatiesystemen die beveiligd moeten worden om de werking van Defensie zoveel mogelijk ongestoord doorgang te laten vinden of als aantasting hiervan de belangen van de Nederlandse Staat of Defensie kunnen schaden.” Er worden een 4-tal TBB-en onderkend. Van zeer grote schade, dus zeer vitaal (TBB-1), tot beperkte schade en dus beperkt belangrijk (TBB-4). Daartussen liggen TBB-2 (vitaal/essentieel) en TBB-3 (belangrijk).

De A/006 gaat over de risicoattitude die Defensie hanteert aangaande de TBB-en. Waarbij geldt dat bij TBB-1 en TBB-2 eigenlijk geen restrisico’s worden geaccepteerd en bij TBB-4 schades ongewenst zijn. TBB-3 ligt qua risicoacceptatie daartussen. Deze risicomatrix behandelt niet de kans van optreden maar gaat uit van mogelijke impact. De kans van optreden wordt dus eigenlijk op 100% gezet. De afbeelding hierna geeft dit schematisch weer.

TBB-1	Zeer grote schades voor de NL Staat, Restrisico's worden niet geaccepteerd
TBB-2	Grote schades voor de NL Staat of Defensie, Restrisico's worden in beginsel niet geaccepteerd
TBB-3	Schades voor de NL Staat of Defensie, Restrisico's worden zoveel mogelijk gemitigeerd
TBB-4	Schade voor Defensie, Restrisico's worden zoveel mogelijk gemitigeerd

Figuur 7 - Te Beschermen Belangen (TBB)

De D/101 beschrijft hoe het goedkeuringsproces voor informatie- en OT-systemen moet plaatsvinden. De eerdergenoemde TBB-en worden gebruikt voor de risicoattitude. Daarbinnen moet een specifieke dreigingsanalyse worden uitgevoerd per informatie-, OT-systeem. Soms zitten de risico's primair op ongewenste openbaarwording en soms vooral op de beschikbaarheid van het systeem. In de Statement of Compliance, een document over de verantwoording van de in het beleid bepaalde maatregelen, is hierover een risicomatrix opgenomen. Deze matrix onderkent kans en impact als factoren die gebruikt wordt voor de initiële- en de restrisico-bepaling op basis van de uitgevoerde dreigingsanalyse.

		Impact				
		Zeer laag 1	Laag 2	Midden 4	Hoog 8	Zeer hoog 16
Kans	Zeer hoog 5	5	10	20	40	80
	Hoog 4	4	8	16	32	64
	Midden 3	3	6	12	24	48
	Laag 2	2	4	8	16	32
	Zeer laag 1	1	2	4	8	16

Tabel 3 - Risicomatrix Defensie

Stap 2 – Thema's plotten op de risicomatrix

Vanuit de doelstelling van dit onderzoek kan de kans van optreden in deze fase nog niet kan worden bepaald en wordt die daarom op 100% gezet. Voor het inschatten van categorieën onderkent Defensie een 4-tal TBB-en waardoor de risico-tabel uit Figuur 7 het best past. De risicomatrix uit Tabel 3 valt dus af voor deze casus.

De thema's uit hoofdstuk 3 met bijbehorende sub-thema's en voorbeelden zijn vervolgens langs de voorbeelden uit de A/005 gehouden. Opvallend is dat systemen die een veiligheidsrisico voor mensen hebben een hoger TBB (TBB-3) kennen dan systemen die dat niet hebben (TBB-4) en

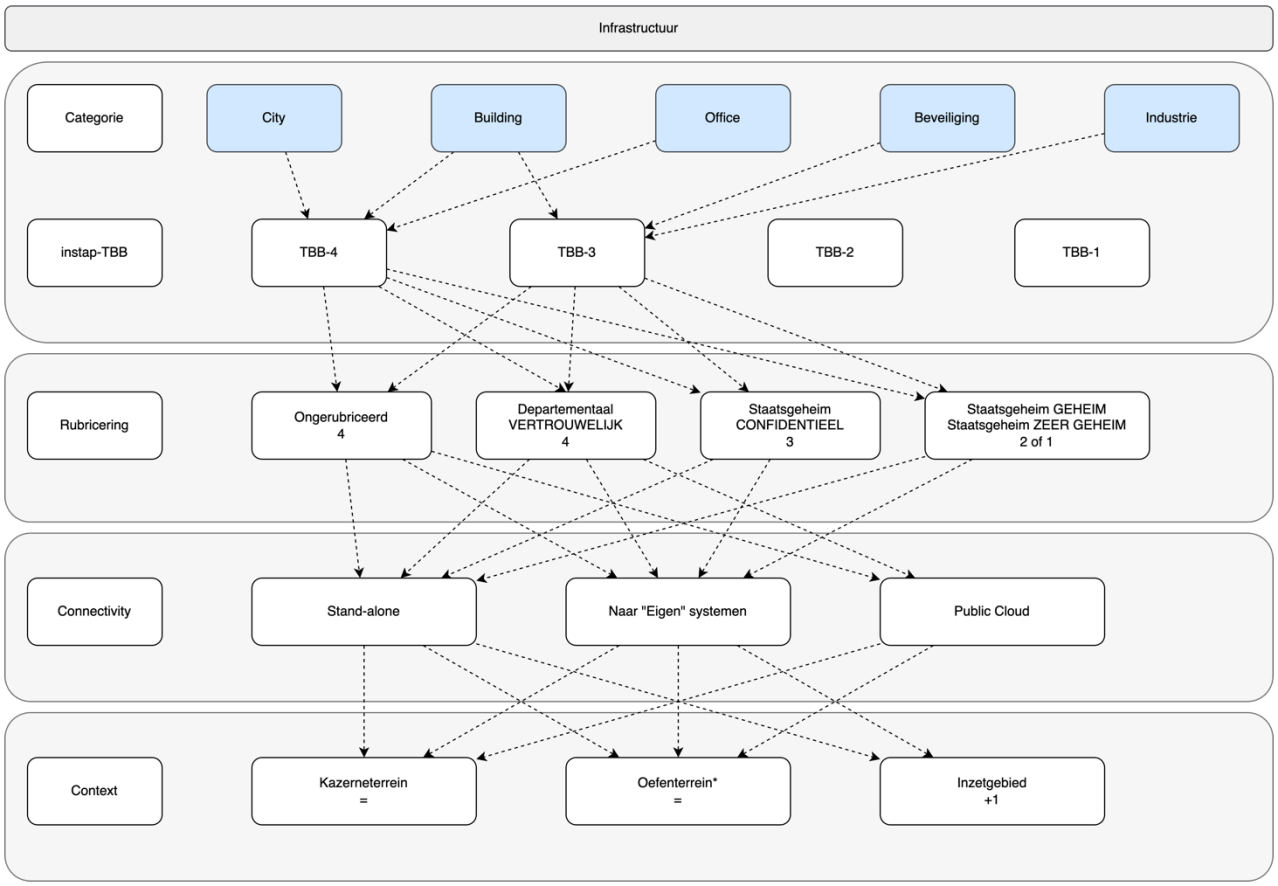
dat sensor-, wapen- en communicatiesystemen vanwege hun directe relatie met de kerntaken van de Krijgsmacht als erg belangrijk worden bestempeld (TBB-2). Figuur 8 geeft de resultaten van deze analyse weer. Hierbij is het belangrijk dat dit het ingangs-TBB is. Dit TBB kan veranderen naargelang de context en de rubricering waarbinnen het smart device moet functioneren.

Thema	Categorie	Voorbeeld
Infrastructuur	City	Energiebeheer (zonnepanelen, laadpalen)
		Parkeerplekbeheer
	Building	Gebouwbeheersing (klimaat, temperatuur)
		Appliances (koelkast, koffiezetapparaat)
		Verlichting
		Bezettingsdetectie
		Brandmeld/blussystemen
	Office	SmartTV's
		VTC
		Smart (white)boards
	Beveiliging	CCTV
		Detectiesystemen (lussen, PIR-etjes)
	Industrie	Plant control
		Proces Control
		Machinecontrol
		(olie)pijpleidingen
Militair Materieel	SeWaCo	MQ9
		F35
		RWCS (Remote Controlled Weapon Stations)
		APS (Armour Protection Systems)
		Smart munitie
		Radar
		Sonar
	Transport	Voertuigen (vrachtwagen, auto)
		Containers
		Shovels
		Onbemande voertuigen (THeMIS)
		Transport drones
Persoonsgebonden	Health	Hoortoestellen
		Implantaten (pacemakers, insulinepompen)
		Body Area Network systemen (smart pills)
		Smart watches (activity trackers)
	Mobiele devices	Smartphones
		Tablets

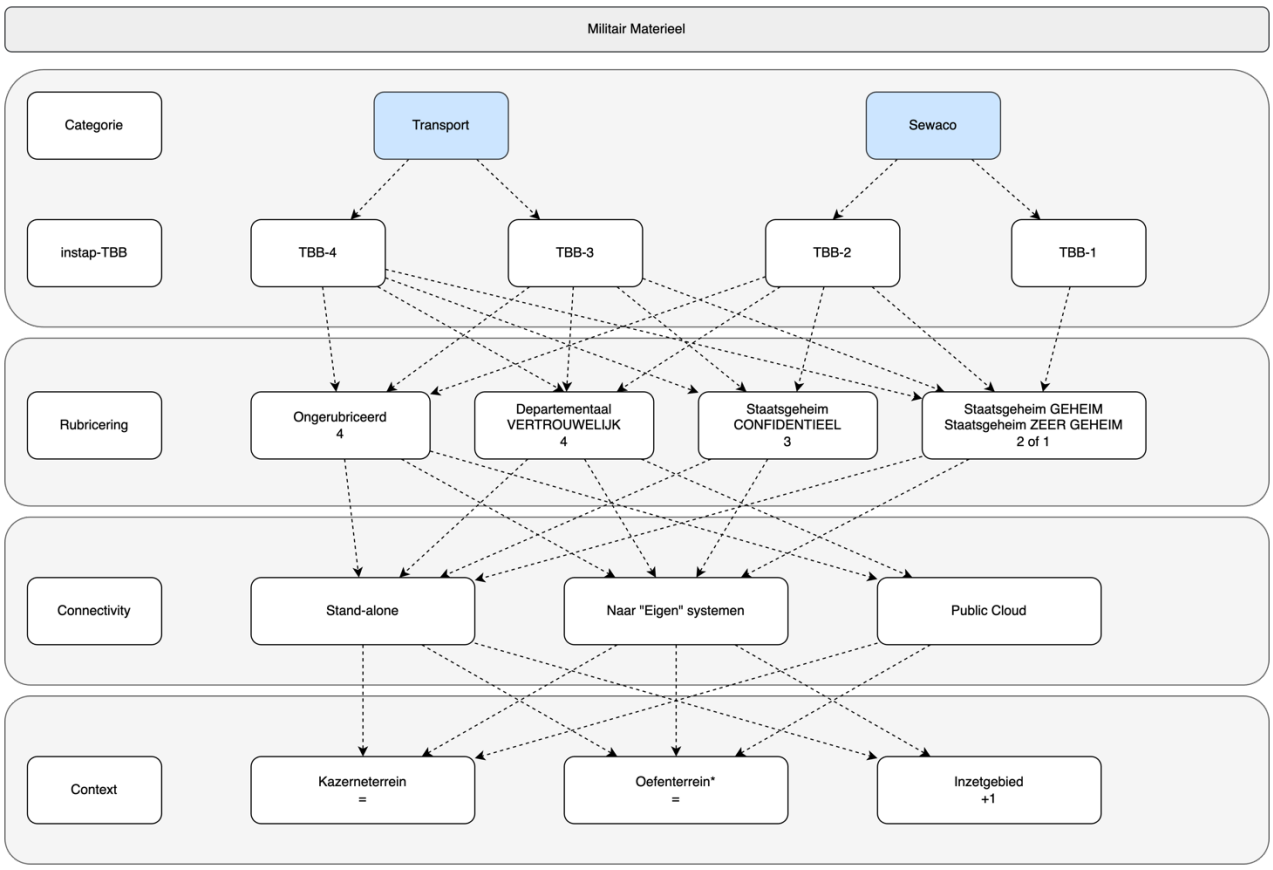
NOT FOR PUBLIC RELEASE

Figuur 8 - Thema's gekoppeld aan TBB

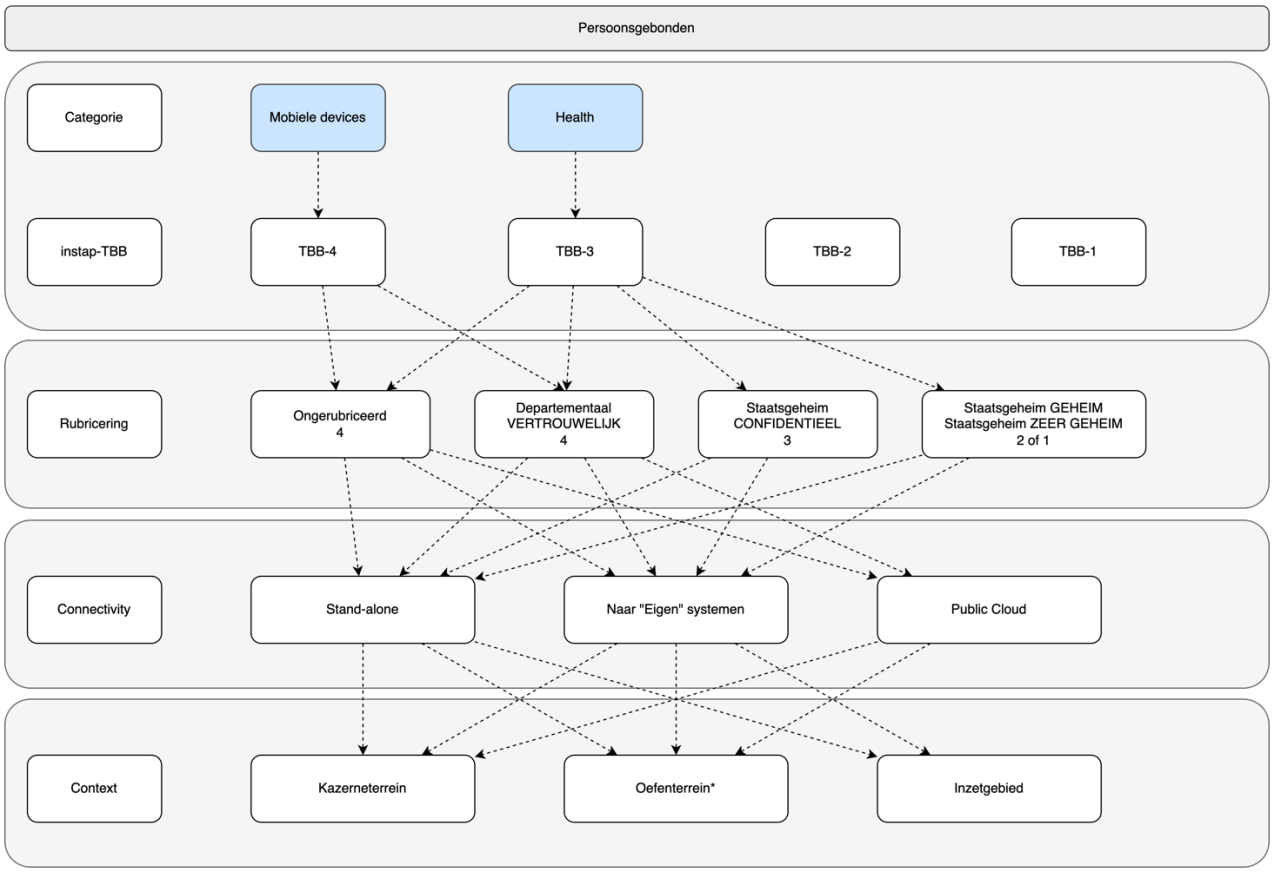
Stap 3 – In deze stap zijn de risicocriteria uit hoofdstuk 4 gekoppeld en per thema verwerkt in een model. Nu de Thema's, sub-thema's en voorbeelden zijn gekoppeld aan de ingangs-TBB-en is de context, de rubricering en de mogelijke opties daartussen in kaart gebracht. Zo is het bijvoorbeeld wel mogelijk om een smart-TV op een kazerne in een ongerubriceerde omgeving wel te koppelen aan een public Cloud maar is dit absoluut geen optie voor diezelfde TV tijdens een missie in een inzetgebied. Figuren 8, 9 & 10 geven de mogelijke opties per thema en categorie weer.



Figuur 9 - Smart infrastructuur



Figuur 10 – Smart militair materieel



Figuur 11 - Persoonsgebonden smart devices

Klankbordgroep: Deze bevindingen zijn gepresenteerd aan de klankbordgroep. Daarbij zijn ook de genade aannames voor de totstandkoming van bovengenoemde modellen vermeld.
De aannames die gebruikt zijn voor de totstandkoming zijn:

- Grote risico's betekenen een hoog belang voor de organisatie en dat betekent dat een goede beheersing noodzakelijk is;
- Dat kleine risico's een laag belang voor de organisatie kennen en dus betekent dat een beperkte beheersing volstaat;
- Dat beheersing en verantwoording over de risico's in lijn zijn met bovenstaande punten.

De klankbordgroep was het – na een goede discussie – unaniem eens met de gedane analyse en de ingenomen standpunten/aannames.

6.4 Conclusies

Na het bestuderen van Defensie's interne documenten aangaande beveiliging viel op dat zij een 4-tal risicocategorieën onderkent. Defensie noemt dit Te Beschermen Belangen (TBB). Deze TBB-gedachte heeft Defensie verder verwerkt in concrete voorbeelden (A/005) en hebben hier een risicoattitude aan gekoppeld (A/006). Na bestudering van genoemde voorbeelden in A/005

bleek er een trend te herkennen tussen de belangen die Defensie hecht aan wapensystemen, veiligheid en standaardsystemen. Deze trend is hieronder weergegeven.

- TBB-4 – Standaard Te Beschermen Belang;
- TBB-3 – Systemen waarbij Safety of Security in het geding kan zijn;
- TBB-2 – Systemen die de vitale belangen van de organisatie raken.

Ook speelt de rubricering van een rol in het uiteindelijke TBB.

Door het bestaan van deze methodiek was het mogelijk om de categorieën smart devices te koppelen aan deze TBB-en en dit te bespreken met de klankbordgroep om de aannames en analyses te toetsen en te valideren.

7 Conclusies en aanbevelingen

Na beantwoording van alle deelvragen is het nu tijd om de hoofdvraag “Welke elementen zijn van belang zodat Defensie de beveiligingsrisico’s van smart devices op voorhand kan inschatten en op een passende wijze beheersen?” te beantwoorden.

7.1 Samenvatting onderzoek

Dit onderzoek is begonnen met de vraag wat een smart device is. Een vraag die in eerste instantie eenvoudiger te beantwoorden lijkt dan dat dat in werkelijkheid het geval is. De gevonden onderzoeken op het gebied van smart devices bevinden zich allemaal in het paradigma van het Internet of Things (IoT). IoT en smart device worden dan ook meestal als synoniemen van elkaar gebruikt. Toch bevinden zich niet alle devices binnen het paradigma van IoT. Een auto bijvoorbeeld hoeft niet verbonden te zijn om toch smart te zijn. Denk bijvoorbeeld aan een collision avoidance systeem, rijstrookassistentie en vermoeidheidsdetectie. Smartness heeft te maken met “ontzorgen” en het verhogen van de kwaliteit van leven. Dat kan bijvoorbeeld op het gebied van comfort, beveiliging, veiligheid en interactie met anderen zijn. De manier waarop dat gebeurt kan variëren van een eenvoudige beslisboom tot aan het gebruik van Artificial intelligence (AI). De volgende definitie is gekozen voor een smart device: *“Een smart device is omgevingsbewust, autonoom, kan leren via algoritmes en/of software updates en staat eventueel in verbinding met andere apparaten en/of systemen.”*

Nadat de definitie is bepaald is onderzocht welke categorieën smart devices er te onderkennen zijn bij Defensie. Dat is gedaan door de literatuur hierover te bestuderen en voor het Defensiespecifieke deel zijn interviews gehouden. Op basis hiervan is een model ontwikkeld dat alle gevonden categorieën heeft weten samen te voegen tot een 3-tal thema’s. Smart infrastructure, militair materieel en persoonsgebonden devices. Binnen deze thema’s zijn sub-thema’s met voorbeelden gedefinieerd. Hierbij is de balans gezocht tussen groeperen en specificeren om te voorkomen dat het model te algemeen wordt om waardevol te zijn.

Onderzocht is eveneens welke criteria van belang zijn om te komen tot een goede risicobeoordeling op smart devices. Naast bestudering van de literatuur is ook hier gebruik gemaakt van het interview. Gevonden risico’s komen neer op beveiligings- en veiligheidsrisico’s. Goed is op te merken dat het doel, de kans, van het smart device ook wordt meegenomen in de afweging. De risico’s gaan vooral over de beheersbaarheid en de mogelijke consequenties als het fout gaat.

Uiteindelijk zijn er een 3-tal criteria van belang om te komen tot een goede risicobeoordeling. Dit zijn Type smart device, context en rubricering.

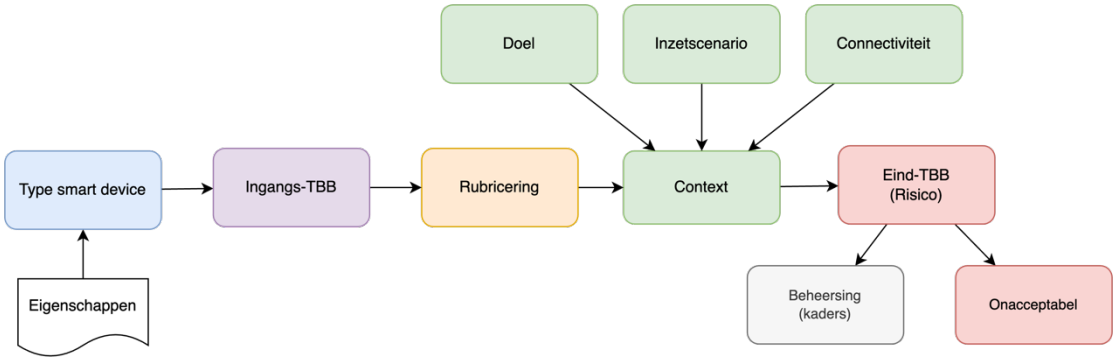
Voor de beheersing van de risico's is onderzocht welke kaders beschikbaar zijn voor de beheersing van smart devices. Bestaande kaders voor IT lijken niet goed te passen op smart devices. Het is bijvoorbeeld niet echt mogelijk om antivirussoftware te installeren in een auto of een robotstofzuiger. Uiteindelijk zijn er 3 kaders gevonden die geschikt zijn voor de Europese markt. De IEC 62443, een kader voor de industrie, de ETSI EN 303 645, een kader voor consumentenelektronica en tot slot de ISO/IEC 27400 een kader voor de beveiliging en privacy van IoT.

Voor het plotten risicobeoordelingen voor smart devices op de bij Defensie in gebruik zijnde risicomatrixen is gebruik gemaakt van de gevonden resultaten aangaande categorieën smart devices en de risicocriteria. Ook is er een documentenonderzoek uitgevoerd binnen Defensie. Vanuit die resultaten is een model ontworpen. Dit model is voorgelegd aan de klankbordgroep ter validatie. De deelnemers van de klankbordgroep waren unaniem akkoord met het gepresenteerde model, de afwegingen die bij de totstandkoming zijn gemaakt en de aannames die zijn gedaan.

7.2 Conclusies

7.2.1 Beantwoording hoofdvraag

Met de resultaten van de deelvragen samengevoegd kan de hoofdvraag beantwoord worden. "Welke elementen zijn van belang zodat Defensie de beveiligingsrisico's van smart devices op voorhand kan inschatten en op een passende wijze beheersen?" Deze vraag kan worden beantwoord door middel van een model en methode. Het hiervoor ontwikkelde model en methode wordt uitgewerkt in een instrument. Defensie moet hiervoor nog de keuze maken met welk(e) kader(s) ze dat willen doen. Het finaliseren van het instrument paste (helaas) niet meer binnen de periode van dit onderzoek en is daarom buiten de scope van deze thesis geplaatst.



Figuur 12 - Model risicobeheersing smart devices Defensie

Het hiervoor getoonde model is gebaseerd op de samenvoeging van de deelvragen.

1. Type smart device. Het type smart device heeft een aantal eigenschappen. Standaard, Safety en/of SeWaCo. Dit zijn de eigenschappen die komen uit hoofdstuk 6 en bepalend zijn voor de risicomatrix binnen Defensie;
2. Dit samen bepaalt het ingangs-TBB;
3. De rubricering van de data binnen het smart device of de rubricering van de omgeving waarbinnen het smart device moet functioneren kan van invloed zijn op het eind-TBB.
4. Vervolgens moet de context worden gescoord. Die bestaat uit het doel, het inzetscenario, (kazerne, oefenterrein en/of inzetgebied) en de connectiviteit (moet het gekoppeld worden met een netwerk).
5. Al deze zaken samen vormen het Eind-TBB. Op basis hiervan wordt een besluit genomen. Onacceptabel betekent dat de risico's (veel) groter zijn dan de benefits.
6. Beheersing gaat over de benodigde kaders voor het smart device. Dat kunnen standaard kaders zijn of specifieke kaders. (Hierover moet nog besloten worden).

De methode bij dit model zal een (op Excel) gebaseerd document zijn die gepubliceerd zal worden op een centrale plek op het intranet. Dit instrument zal de medewerker in staat moeten stellen om op basis van een self-assessment tot een advies te komen. Dit model biedt alleen een oplossing voor nog aan te schaffen smart devices. Smart devices die al binnen de organisatie zijn worden niet door dit model geraakt.

Als we de vrachtwagen uit de probleemcontext (par.1.2) langs het model zouden leggen dan zou die een ingangs-TBB krijgen van TBB-3. De vrachtwagen in deze casus rijdt standaard in een ongerubriceerde context maar zou wel overal ingezet kunnen worden van kazernes, tot aan missiegebieden. Op basis van deze kenmerken wordt het eind TBB van deze vrachtwagen TBB-2. In de praktijk betekent dit dat een beveiligingscoördinator met de behoeftesteller meekijkt en -denkt. Bij missiegebieden is connectiviteit naar de public cloud sowieso geen optie dus daar kan bij de offerteaanvraag in het aanbestedingstraject rekening mee worden gehouden. De beheersing van de cyberrisico's zou op basis van de IEC 62443 kunnen geschieden. Een tweede hypothetisch voorbeeld zou de aanschaf van een smart-TV kunnen zijn. Deze TV heeft standaard het TBB-4. De TV wordt ingezet in een ruimte op een kazerneterrein waar ook met geheime informatie wordt gewerkt. De TV mag op basis van de rubricering alleen verbinding leggen met "Eigen" systemen. Dat betekent dus dat alle draadloze modules (Bluetooth en WiFi) uit de TV moeten zijn verwijderd voordat deze de ruimte in mag. Het eind TBB wordt TBB-2. Beheersing van de cyberrisico's zou

kunnen gebeuren door de maatregelen uit het DBB eventueel aangevuld met een conformancy statement op basis van het ETSI EN 303 645 framework.

Het model/methodiek biedt geen oplossing voor privé-middelen die de Defensiemedewerker introduceert bij Defensie. Hieronder vallen dus auto's met camera's die Defensieterreinen oprijden maar ook de smart-home apparatuur die indirect wordt geïntroduceerd bij het (hybride) thuiswerken. Of het wenselijk is om als werkgever daar iets van te vinden ligt buiten de scope van deze thesis en is aan de werkgever om verder te onderzoeken.

7.2.2 Wetenschappelijke reflectie

Smart technologie wordt steeds vaker onderzocht in de wetenschap. Wel vooral binnen het paradigma van het Internet of Things. Op basis van dit onderzoek is gebleken dat er binnen de literatuur nog geen consensus is over wat nu precies een smart device is. Dat heeft mogelijk te maken met de grote technologische ontwikkelingen op dit vlak. Zo worden er met grote regelmaat nieuwe smart technologieën geïntroduceerd. Smartness varieert qua techniek momenteel van een eenvoudige beslisboom tot aan AI. Deze ontwikkelingen hebben elkaar in een relatief kort tijdbestek opgevolgd. Wetenschappers zoals Manuel Silvério-Fernandez en Sebastian Fischer hebben getracht de eerste stappen te zetten om een definitie, categorisering en beheersing van smart devices te beschrijven. Van hun werk is in dit onderzoek dankbaar gebruik gemaakt en op doorgebouwd. Natuurlijk moet wel rekening worden gehouden met de beperkingen die een Masterthesis met zich meebrengt in doorlooptijd en dus de daarmee gepaarde diepgang. Toch ben ik van mening dat – gegeven de huidige staat van de techniek – de thesis voldoende handvatten zou moeten bieden om Defensie te helpen met het vaststellen van de risico's en ze te adviseren over de beheersing ervan. Helaas biedt die geen garanties voor nieuwe technologieën want onbekend is nog wat die gaan zijn en hoe disruptive die mogelijk is. Er is wel wetgeving onderweg zoals bijvoorbeeld de Cyber Resillience Act en de AI-act die in ieder geval wat kaders meegeven rondom de beveiliging en de uitlegbaarheid van AI.
Ook op het gebied van beheersing is niet meteen duidelijk welke koers gevaren moet worden. Veel wetgeving is onderweg maar is er dus nog niet. Zomaar een beheersingsframework eisen is dus mogelijk iets waarop de markt nog niet is ingespeeld en dus bij offerteaanvragen mogelijk voor nare verrassingen kan leiden omdat je mogelijk te ver voor de muziek vooruit loopt.

7.3 Aanbevelingen

Deze paragraaf beschrijft de aanbevelingen voor de organisatie en voor de wetenschap en dan vooral op het gebied van mogelijke vervolgonderzoeken.

7.3.1 Voor de organisatie

De tijden dat Defensie 1 grote ommuurde tuin was met maar één digitale toegangspoort is met de introductie van het Internet of Things verleden tijd. Met steeds grotere regelmaat worden apparaten geïntroduceerd die rechtstreeks verbonden zijn aan het internet en voorzien zijn van allerlei sensoren. Dit introduceert nieuwe aanvalsoppervlakken voor de organisatie waarvoor de standaard normenkaders bij Defensie niet dekkend genoeg zijn. Hoog tijd dus voor een robuust normenkader dat Defensie in staat stelt om af te rekenen met deze zogenaamde Shadow IT en in control te raken over wat de organisatie binnenkomt. Hieronder volgen daarom een paar aanbevelingen voor de organisatie om dat te realiseren.

Maak een keuze voor een framework dat past bij wat de markt kan en wat Defensie nodig heeft. De veiligste keuze voor Defensie is de IEC 62443. Dat is een zeer uitgebreid normenkader - bedoeld voor de industrie - met voldoende waarborgen voor de beheersing van smart devices. Een keuze voor dat normenkader betekent echter zeer waarschijnlijk dat er een inkoop-infarct ontstaat omdat behoeftes niet (tijdig) kunnen worden ingevuld omdat de markt het normenkader niet kent en geen offerte wil uitbrengen of veel tijd nodig heeft om zich te kunnen verantwoorden aan dat kader. De ETSI EN 303 645 is voornamelijk gericht op consumenten IoT en doet waarschijnlijk geen recht aan de noden van een Defensieorganisatie. De ISO 27400 kan beide domeinen afdekken maar is wellicht zo nieuw dat de markt daar ook geen antwoord op heeft.

1. Ontwikkel een informatiecampagne over de risico's van smart devices bij Defensie om awareness bij de medewerkers te creëren.
2. Beproef de IEC 62443 voor apparatuur binnen het thema "Militair materieel" op een beperkt aantal trajecten en meet de resultaten op het gebied van doorlooptijd en haalbaarheid. Op basis van de behaalde resultaten kan het kader worden vastgesteld of moet worden gezocht naar een alternatief.
3. Beproef de ETSI EN 303 645 bij de aankoop van een beperkt aantal smart appliances in een gerubriceerde context. Meet ook hier de resultaten en evalueer na afloop van de meetperiode over de haalbaarheid.

De prioriteiten van deze aanbevelingen zijn op basis van de nummering aangegeven. De belangrijkste aanbeveling als eerst. De minder belangrijke aanbeveling als laatst.

7.3.2 Voor de wetenschap

Wat dit onderzoek heeft laten zien is dat er nog veel kennis te behalen is binnen het thema smart devices.

Vervolgonderzoek is in ieder geval nodig op het gebied van:

- Categorieën smart devices: Op basis van de huidige gevonden literatuur kan worden gesteld dat de onderzoeken op dat vlak te algemeen zijn om waardevol te zijn op het gebied van beheersing en risico-inschatting.
- Normenkaders: Er zijn een aantal normenkaders en consumentenlabels gevonden. Het eenvoudige feit dat experts binnen het vakgebied geen goede labels en normenkaders konden noemen laat zien dat er nog veel te winnen is op dat vlak. Onderzoek naar de volwassenheid van de markt rondom de in gebruik zijnde normenkaders zou een waardevolle aanvulling kunnen zijn op dit onderzoek en zou kunnen laten zien of de markt zichzelf al aan het organiseren is op dit vlak of dat wetgeving pas een motivatie is om een veilig product te creëren en te leveren.
- Cybersecurity: Naast theoretische onderzoeken zouden praktische technische security assessments op smart devices ook een actueel inzicht kunnen bieden rondom de beveiliging en kwetsbaarheden binnen smart devices.

Literatuurlijst

AIVD. (z.d.). *Wat is een offensief cyberprogramma?* Geraadpleegd 16 augustus 2023, van https://www.aivd.nl/onderwerpen/cyberdreiging/vraag-en-antwoord/wat-is-een-offensief-cyberprogramma

Albayaydh, W. S., & Flechais, I. (2022, april 29). Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3491102.3502097

Aly, M., Khomh, F., & Yacout, S. (2021). What Do Practitioners Discuss about IoT and Industry 4.0 Related Technologies? Characterization and Identification of IoT and Industry 4.0 Categories in Stack Overflow Discussions. *Internet of Things*, *14*, 100364. https://doi.org/10.1016/j.iot.2021.100364

Apple. (2023, juli 24). *Over software-updates voor HomePod*. https://support.apple.com/nl-nl/HT208714

Autoblog.nl. (2020, februari 6). *Nederlandse BMW 7 crasht, belt zelf hulpdiensten*. https://www.autoblog.nl/nieuws/nederlandse-bmw-7-crasht-belt-zelf-hulpdiensten-139267

Bassi, A., & Horn, G. (2008). *Internet of Things in 2020: Roadmap for the future*.

Boeije, H. (2009). *Analysis in qualitative research.* . SAGE Publications.

Cao, X., & Liu, L. (2020). Use of Smart Devices: A Survey, Some Research Issues, and Challenges. *Proceedings - 2020 International Conference on Culture-Oriented Science and Technology, ICCST 2020*, 378–382. https://doi.org/10.1109/ICCST50977.2020.00079

Centrum voor Informatiebeveiliging & Privacy. (2023). *Baseline Informatiebeveiliging Overheid*. https://bio-overheid.nl/

CSA Singapore. (z.d.). *Cybersecurity Labelling Scheme (CLS) For Manufacturers*. Geraadpleegd 6 oktober 2023, van https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers

Cybersecurity Certification Centre. (z.d.). *Cybersecurity Certification Guide*.

Danev, V., Kirilov, L., & Nikolov, R. (2021). Creating smart home environment based on open source home automation software. *ACM International Conference Proceeding Series*, 81–86. https://doi.org/10.1145/3472410.3472444

De Souza, B. P., Motta, R. C., & Travassos, G. H. (2019). Towards the description and representation of smartness in IoT scenarios specification. *ACM International Conference Proceeding Series*, 511–516. https://doi.org/10.1145/3350768.3351797

ETSI. (2020). *EN 303 645 - V2.1.1 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*.

European Commission. (2014). *Radio Equipment Directive (RED)*. https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

Europees Parlement en de Raad. (2019). *Verordening 2019/2144 - Voorschriften voor de typegoedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd wat de algemene veiligheid ervan en de bescherming van de inzittenden van voertuigen en kwetsbare weggebruikers betreft*. https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/vademecum_2018.pdf

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). *Foundational cybersecurity activities for IoT device manufacturers*. https://doi.org/10.6028/NIST.IR.8259

Fischer, S. (2022). *Internet of Things: A Model for Cybersecurity Standards and the Categorisation of Devices*. https://doi.org/10.17169/refubium-36965

Fischer, S., Neubauer, K., & Hackenberg, R. (2020). A Study about the Different Categories of IoT in Scientific Publications. In *CLOUD COMPUTING 2020: the Eleventh International Conference on Cloud Computing, GRIDs and Virtualization* (pp. 24–30).

Fournier, H., Kondratova, I., & Katsuragawa, K. (2021). *Smart Technologies and Internet of Things Designed for Aging in Place* (pp. 158–176). https://doi.org/10.1007/978-3-030-77392-2_11

Gochoo, M., Alnajjar, F., Tan, T.-H., & Khalid, S. (2021). *Towards Privacy-Preserved Aging in Place: A Systematic Review*. https://doi.org/10.3390/s21093082

Great Britain. Department for Digital, C. (2020). *Government response to the 'Regulatory proposals for consumer Internet of Things (IoT) security' consultation.* Stationery Office.

Houze, E., Diaconescu, A., Dessalles, J. L., & Menga, D. (2022). A generic and modular reference architecture for self-explainable smart homes. *Proceedings - 2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems, ACSOS 2022*, 101–110. https://doi.org/10.1109/ACSOS55765.2022.00028

Howell, G., Franklin, J. M., Sritapan, V., Souppaya, M., & Scarfone, K. (2023). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. https://doi.org/10.6028/NIST.SP.800-124r2

ISA Global Security Alliance. (2023). *Quick Start Guide: An Overview of ISA/IEC 62443 Standards, Security of Industrial Automation and Control Systems*. www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

K., I., & M., A. K. (2019). A Study on Machine Learning Techniques for Internet of Things in Societal Applications. *2019 International Conference on Data Science and Communication (IconDSC)*, 1–6. https://doi.org/10.1109/IconDSC.2019.8816970

Khalid, K., & Madi, E. N. (2020). A review of computation offloading for mobile cloud computing based on fuzzy set theory. In *International Journal of Engineering Trends and Technology* (Nummer 1, pp. 56–63). Seventh Sense Research Group. https://doi.org/10.14445/22315381/CATI3P209

Koolen, C. (2021). Cybersecurity voor het Internet of Things: Hoe beoordeel je de juridische gevolgen van slimme apparaten met beveiligingsproblemen? *Cybersecurity Research Vlaanderen*.

Llanez-Caballero, I., Ibarra, L., Peña-Quintal, A., Catzín-Contreras, G., Ponce, P., Molina, A., & Ramirez-Mendoza, R. (2023). The “Smart” Concept from an Electrical Sustainability Viewpoint. In *Energies* (Vol. 16, Nummer 7). MDPI. https://doi.org/10.3390/en16073072

Maestre-Gongora, G., Fernando Colmenares-Quintero, R., & Stansfield, K. (2020). *Mapping concept and challenges for smart technologies: a systematic study approach*. http://www.aisti.euNºE32

Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*.

Ministerie van Defensie. (2019). *Algemene Beveiligingseisen voor Defensieopdrachten 2019*. https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2020/02/04/abdo-2019/ABDO2019_Definitief_V1.1_web.pdf

Ministerie van Defensie. (2022, juli 1). *Het verhaal van Defensie | Aantallen personeel*. https://www.defensie.nl/onderwerpen/overdefensie/het-verhaal-van-defensie/aantallen-personeel

Mozilla Foundation. (2023, september 6). *It’s Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

Najjar, Y. S. H., & Bani Amer, M. M. (2016). Using a smart device and neuro-fuzzy control system as a sustainable initiative with green cars. *Journal of the Energy Institute*, *89*(2), 256–263. https://doi.org/10.1016/j.joei.2015.01.021

NCSC. (2023). *Basis-beveiligingsmaatregelen slimme apparaten (IoT)*.

Ndunagu, J. N., Ukhurebor, K. E., Akaaza, M., & Onyancha, R. B. (2022). Development of a Wireless Sensor Network and IoT-based Smart Irrigation System. *Applied and Environmental Soil Science*, *2022*, 1–13. https://doi.org/10.1155/2022/7678570

Pallavi, B., Othman, B., Trivedi, G., Manan, N., Pawar, R. S., & Singh, D. P. (2022). The Application of the Internet of Things (IoT) to establish a technologically advanced Industry 4.0 for long-term growth and development. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022*, 1927–1932. https://doi.org/10.1109/ICACITE53722.2022.9823481

Parhusip, H. A., Trihandaru, S., Rumaksari, A. N., Puspitasari, M. D., Haryadi, A. H., & Santosa, P. P. (2022). Integrated Sensors into Artificial IntelligenceMining(AI-Mining) Data Acquisition of Environmental Features; Integrated Sensors into Artificial IntelligenceMining(AI-Mining) Data Acquisition of Environmental Features. *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*. https://doi.org/10.1109/IIHC55949.2022.10060158

Rijksinspectie Digitale Infrastructuur (RDI). (z.d.). *Tips voor beveiliging slimme apparaten | Tips voor veilig gebruik van apparaten*. Geraadpleegd 8 oktober 2023, van https://www.rdi.nl/onderwerpen/tips/beveiliging-slimme-apparaten

Rijksoverheid. (z.d.). *Zakendoen met Defensie*. Geraadpleegd 16 september 2022, van https://www.rijksoverheid.nl/ministeries/ministerie-van-defensie/contact/zakendoen-met-defensie

Rijksoverheid. (1815, augustus 24). *Grondwet*. https://wetten.overheid.nl/BWBR0001840/2022-08-30/0

Rijksoverheid. (2013). *Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)*. https://wetten.overheid.nl/BWBR0033507/2013-06-01

Rijksoverheid. (2022). *Wetboek van Strafrecht*. https://wetten.overheid.nl/BWBR0001854/2022-10-01

Rijksoverheid. (2023, juli 19). *Brussel zet stap richting veiligere digitale producten*. https://www.rijksoverheid.nl/actueel/nieuws/2023/07/19/brussel-zet-stap-richting-veiligere-digitale-producten

Risteska Stojkoska, B. L., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. In *Journal of Cleaner Production* (Vol. 140, pp. 1454–1464). Elsevier Ltd. https://doi.org/10.1016/j.jclepro.2016.10.006

Sami, S., Dai, Y., Tan, S. R. X., Roy, N., & Han, J. (2020). Spying with your robot vacuum cleaner. *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 354–367. https://doi.org/10.1145/3384419.3430781

Schindler, P. S. (2019). *Business Research Methods* (13th dr.). McGraw-Hill.

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2022). The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance. *International*

Journal of Human-Computer Interaction, *38*(13), 1276–1289. https://doi.org/10.1080/10447318.2021.1994211

Sepasgozar, S., Karimi, R., Farahzadi, L., Moezzi, F., Shirowzhan, S., M. Ebrahimzadeh, S., Hui, F., & Aye, L. (2020). A Systematic Content Review of Artificial Intelligence and the Internet of Things Applications in Smart Home. *Applied Sciences*, *10*(9), 3074. https://doi.org/10.3390/app10093074

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. In *IEEE Communications Surveys and Tutorials* (Vol. 23, Nummer 2, pp. 1125–1159). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2021.3064507

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2019). Evaluating critical success factors for implementing smart devices in the construction industry. *Engineering, Construction and Architectural Management*, *26*(8), 1625–1640. https://doi.org/10.1108/ECAM-02-2018-0085

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2021). Strategic framework for implementing smart devices in the construction industry. *Construction Innovation*, *21*(2), 218–243. https://doi.org/10.1108/CI-11-2019-0132

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, *6*(1), 3. https://doi.org/10.1186/s40327-018-0063-8

SonicWall. (2023a). *Cyber Threat Report*.

SonicWall. (2023b). *Mid-Year Update: Cyber Threat Report*.

Staveren, M. Th. van. (2015). *Risicogestuurd werken in de praktijk*. Vakmedianet.

Subramanian, G., & Nagabushanam, H. (2022). Governance of Data Product in Multi-layered IoT system. *International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2022*. https://doi.org/10.1109/ICECCME55909.2022.9987960

Taleb, N. N. (2016). *De Zwarte Zwaan, De impact van het hoogst onwaarschijnlijke* (Tweede edi). Uitgeverij Nieuwezijds.

Tesla. (z.d.). *Autopilot en Full Self-Driving Capability | Tesla Support Nederland*. Geraadpleegd 16 april 2023, van https://www.tesla.com/nl_nl/support/autopilot

The New York Times. (2016, juli 11). *Pokémon Go Brings Augmented Reality to a Mass Audience*. https://www.nytimes.com/2016/07/12/technology/pokemon-go-brings-augmented-reality-to-a-mass-audience.html

van Deursen, A. J. (2021). *Internet- en Internet of Things-vaardigheden in Nederland anno 2021*. 38.

van Deursen, A. J., & Mossberger, K. (2018). Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills. *Policy & Internet*, *10*(2), 122–140. https://doi.org/10.1002/poi3.171

Van Kranenburg, R. (2008). *Repositorium für die Medienwissenschaft The Internet of Things. A Critique of Ambient Technology and the All-seeing Network of RFID 2007*. https://doi.org/10.25969/mediarep/19293

Verschuren, P., & Doorewaard, H. (2021). *Het ontwerpen van een onderzoek* (zesde druk). Boom uitgevers.

Vodă, A. D. S., Tudor, A. I. M., Chiţu, I. B., Dovleac, L., & Brătucu, G. (2021). IoT technologies as instruments for SMEs' innovation and sustainable growth. *Sustainability (Switzerland)*, *13*(11). https://doi.org/10.3390/su13116357

Volk, V., Prange, S., & Alt, F. (2022). PriCheck– An Online Privacy Assistant for Smart Device Purchases. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–5. https://doi.org/10.1145/3491101.3519827

Volvo. (z.d.). *De volledig elektrische Volvo EX90 7-zits SUV | Volvo Cars Nederland*. Geraadpleegd 16 april 2023, van https://www.volvocars.com/nl/cars/ex90-electric/

Wu, C.-Y., & Huang, K.-H. (2020). A Framework for Off-Line Operation of Smart and Traditional Devices of IoT Services. *Sensors*, *20*(21), 6012. https://doi.org/10.3390/s20216012

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

Figuren en tabellen

Figuren

Tabellen

Bijlage A Vragenlijst interview

Een ‘slim’ apparaat of smart device is een omgevingsbewust elektronisch apparaat dat in staat is om zelfstandig beslissingen te nemen en in de meeste gevallen communiceert met andere apparaten en/of mensen.

1. Kun je je vinden in deze definitie?
    a. Waarom wel/niet?
2. Heb je ervaring met (de introductie van) smart devices op de werkvloer?
    a. Zo ja, welke apparaten of welk type apparaten ben je tegengekomen?
3. Denk je dat er bij Defensie types smart devices zouden kunnen voorkomen die niet in de burgermaatschappij voorkomen en omgekeerd?
4. Zie je kansen voor de organisatie door introductie van smart devices?
    a. Zo ja, waarom wel?
    b. Zo nee, waarom niet?
5. Zie je beveiligings-, veiligheidsrisico’s voor de organisatie bij de introductie smart devices?
    a. Zo ja, welke zie je?
    b. Zo nee, waarom niet?
6. Welke criteria hanteer je of zou je kunnen/willen hanteren om risico’s te kunnen inschatten bij smart devices?
7. Is het type smart device naar jouw mening relevant voor de inschatting van risico’s?
    a. Zo ja, gebruik je dan dezelfde criteria (zoals genoemd in de vorige vraag) of komen hier andere criteria bij?
    b. Zo nee, waarom niet?
8. Zijn er – naar jouw weten – (tactische) normenkaders die bestuurders in staat stellen om risico’s rondom smart devices (beleidsmatig) te beheersen?
    a. Zo ja, welke ken je?
9. Zijn er – naar jouw weten – voor “medewerkers” hulp-kaders beschikbaar om op een “Safe for Work”-apparaat te kopen?
    a. Zo ja, welke ken je?
    b. Hoe kan een “medewerker” dat herkennen?
10. Als voor de ‘medewerker’ een instrument ontwikkeld wordt waarmee deze medewerker in staat is om een self-assessment te doen voor aanschaf van een smart device, welke criteria zijn dan volgens jou van belang voor het instrument?
11. Heb je zaken gemist die je graag zou willen bespreken over dit onderwerp?