HOGESCHOOL UTRECHT

Digitale Veiligheid Reservisten

Auteurs
Anke van Gorp, Laura Brands, Kim My Tran, Martine Groen in samenwerking met Maarten Timmerman Sjoerd van Veldhuizen en Pascal Koelmij (Awareways) en Gertjan Dijkstra (CWTC Defensie)

Inlichtingen
anke.vangorp@hu.nl

Datum
27-10-2026

Versie
definitief

© Hogeschool Utrecht,
Utrecht, (27-10-2026)

Bronvermelding is verplicht.
Verveelvoudigen voor eigen gebruik
of interngebruik is toegestaan.

Inhoudsopgave

Inleiding	**3**
Geleerde lessen	**5**
Aanbevelingen	**10**
Aandachtspunten en vervolg	**11**
Bijlage 1 Visuals	**13**
Bijlage 2 Mechanisms of Action en Behavioral Change Techniques	**16**
Bijlage 3 Verantwoording	**22**
Bijlage 4. Juridisch Onderzoek	**33**
Bijlage 5: Literatuurlijst	**59**

© Hogeschool Utrecht, 2026

Inleiding

Digitaal gedrag van medewerkers heeft een grote invloed op de digitale veiligheid van een organisatie en diens medewerkers. Dit geldt ook voor digitaal gedrag in het privéleven. Als een medewerker persoonlijke informatie vrijgeeft via social media dan kan die informatie de organisatie waar deze persoon werkt ook kwetsbaar maken. Als een medewerker in de privésfeer wachtwoorden hergebruikt dan doet deze medewerker dat mogelijk ook op het werk. Dit geldt voor alle organisaties en dus ook voor organisaties in het veiligheidsdomein zoals politie, brandweer, penitentiaire inrichtingen en Defensie. Als Defensie de beveiliging van de eigen systemen op orde heeft en medewerkers getraind heeft in het veilig gebruik van deze Defensie systemen, kunnen er nog steeds risico's ontstaan door gedrag van medewerkers in hun privéleven. Zo bleek dat er nog steeds veel persoonsgegevens van Defensiemedewerkers via de Strava app te achterhalen zijn (Vervaart, 2025). Ook via de app Polarsteps waren via een datalek (volgens Follow the Money) of verkeerde instellingen van gebruikers (Polarsteps) gegevens als werkplek en huisadres van militairen in te zien (Van Kessel, Brommersma en Reuver, 2026). Bovendien hergebruiken nog veel mensen hun wachtwoorden, wat leidt tot risico's voor organisaties als deze wachtwoorden in een datalek zitten (Beuth et al., 2025). Digitaal gedrag van personeel van Defensie in de privésfeer brengt dus niet alleen persoonlijke risico's met zich mee maar ook risico's voor Defensie als geheel, en daarmee indirect ook voor de nationale veiligheid.

Reservisten/vrijwilligers (Defensie, politie, brandweer), een groep mensen die naast een baan en een privéleven ook nog een functie in het veiligheidsveld hebben, vormen in dit vraagstuk een extra relevante groep: zij hebben drie contexten waarin ze digitaal gedrag vertonen. Ze hebben een baan waarin ze over het algemeen digitale middelen gebruiken, ze hebben een functie als vrijwilliger of reservist en een privéleven. Het digitale gedrag in de drie contexten is van invloed op de organisatie in het veiligheidsveld maar de veiligheidsorganisatie kan het digitale gedrag van haar reservisten/vrijwilligers in hun andere baan en privéleven niet reguleren.

In dit project hebben we ons gericht op reservisten van Defensie omdat Defensie op dit moment veel meer reservisten aan het werven is. Defensie heeft van de politiek als doel gekregen te groeien naar 100.000 mensen in 2030, waarvan 20.000 reservisten (kamerstuk 33763, 2025). Deze groei zet daarna ook nog door naar 122.000 (Ministerie van Defensie, 2026). Er is geen reden om aan te nemen dat het digitaal gedrag van reservisten anders is dan dat van de beroepsmilitair, maar zoals hierboven al aangegeven hebben reservisten over het algemeen nog een civiele baan en een privé leven. Reservisten zijn over het algemeen minder vaak in de Defensie omgeving dan beroepsmilitairen.[1] Op het moment dat een reservist ingezet wordt door Defensie dan is die een militair en gelden ook de wetten en gedragscode die het gedrag van een militair reguleren, maar de rest van de tijd is een reservist een burger. Defensie kan het digitale gedrag van reservisten in hun civiele baan en privéleven niet of maar zeer beperkt zien en reguleren, terwijl het digitaal gedrag wel degelijk invloed kan hebben op Defensie.

De hoofdvraag is:
Hoe kunnen we voorkomen dat het digitaal gedrag van reservisten in de privésfeer en de andere betrekkingen tot risico's voor Defensie leidt, rekening houdend met individuele rechten en ethiek?

In dit project, uitgevoerd door onderzoekers van de lectoraten Zorg en veiligheid en Cybersecurity van Hogeschool Utrecht en Awareways in samenwerking met het CWTC van Defensie, zijn we op zoek gegaan naar welke beweegredenen en bijbehorende behavioural change technieques (technieken die je kunt gebruiken om mensen te stimuleren tot een verandering in gedrag)

[1] Er zijn ook reservisten die fulltime bij Defensie werken maar dit zijn uitzonderingen.

© Hogeschool Utrecht, 2026

dan tot gedragsverandering zouden kunnen leiden inclusief ethische en juridische grenzen het meest passend zijn bij de doelgroep reservisten van Defensie. Interventies, of campagnes, zijn immers het meest effectief als ze aansluiten bij de beweegredenen van de reservisten en passen binnen de ethische en juridische grenzen.
Op basis van wetenschappelijke literatuur en interviews met experts in gedragsverandering zijn passende en effectieve beweegredenen voor gedragsverandering geïdentificeerd. De ethische grenzen zijn met morele beraden geëxploreerd en de juridische grenzen met juridische onderzoek, zie bijlage 4 voor een verantwoording van het onderzoek.

In het rapport presenteren we eerst de geleerde lessen, aanbevelingen en de aandachtspunten en vervolg. In de bijlages staan de ontwikkelde visuals, een verdieping van de theorie over Mechanisms of Action en Behavioral Change Technieken, het juridische onderzoek en de verantwoording.

© Hogeschool Utrecht, 2026

Geleerde lessen

Beweegredenen en Behavioral Change technieken

Dit onderzoek biedt een aantal potentiële aanknopingspunten om gedragsverandering bij militairen in gang te zetten. De focus lag op het vinden van beweegredenen die tot gedragsverandering kunnen leiden bij reservisten[2]. Vier beweegredenen zijn hierbij veelbelovend. Te weten;

- Kennis (*Knowledge*)
  - Het besef dat iets bestaat
- Waargenomen vatbaarheid/ kwetsbaarheid (*Perceived susceptibility/vulnerability*)
  - De perceptie van de waarschijnlijkheid dat men kwetsbaar is voor een dreiging.
- Overtuigingen over de gevolgen (*Beliefs about consequences*)
  - Overtuigingen over de gevolgen van een bepaald gedrag (d.w.z. opvattingen over wat er door het vertonen van een bepaald gedrag zal worden bereikt en/of verloren gaan, evenals de waarschijnlijkheid dat een bepaald gedrag tot een specifieke uitkomst zal leiden).
- Sociale/ professionele rol & identiteit (*Social/ professional role & identity*.)
  - Een samenhangend geheel van gedragingen en zichtbare persoonlijke eigenschappen van een persoon in een sociale- of werkomgeving.

Dit viertal geeft belangrijke aanknopingspunten voor het inzetten van gedragsverandering bij reservisten. Te beginnen met kennis, het lijkt een open deur maar toch is het belangrijk om het via deze route bevestigd te krijgen. Het is immers lastig, zo niet onmogelijk om gedrag te veranderen of aan te passen wanneer je niet weet wat het gewenste gedrag is en wanneer dit ingezet dient te worden. Met andere woorden het is essentieel dat een reservist weet wat het gewenste digitaal veilige gedrag is en wanneer en hoe dit in te zetten. Al het voorgaande staat of valt met kennis.
Daarnaast lijkt de waarschijnlijkheid dat men kwetsbaar is voor een dreiging van belang. Dit gaat niet alleen over de eigen kwetsbaarheid maar ook over de kwetsbaarheid van naasten. Vooral dat laatste aspect lijkt van belang. Het belang van kwetsbaarheid van naasten staat niet in het gehanteerde model, maar bij het bekijken van de tekstfragmenten behorende bij deze beweegreden komt dit wel duidelijk naar voren. Het gaat dan altijd over "*Veiligheid -van- jezelf of gezin*".
We hebben hier de theorie dus wat aangevuld, zie bijlage 2.
De derde beweegreden gaat over de gevolgen van bepaald gedrag. Dat kan zowel gaan over gedrag dat leidt tot iets verliezen of juist iets bereiken. Met andere woorden deze beweegreden werkt twee kanten op. Het vertonen van onveilig digitaal gedrag kan leiden tot het verlies van iets, bijvoorbeeld de veiligheid van jezelf en/of van een ander. Maar ook dat veilig digitaal gedrag juist kan bijdragen tot verminderde kwetsbaarheid, van jezelf en/of je naasten en/of je werkgever(s) (inclusief Defensie).
Als laatste is sociale/professionele rol & identiteit een belangrijke beweegreden en dus een mogelijk aangrijpingspunt voor gedragsverandering bij reservisten van Defensie. Het reservist zijn is niet alleen een rol of taak, maar is een onderdeel van de identiteit van de reservist dat altijd aanwezig is, ongeacht de context. Dit is een mooi aanknopingspunt voor gedragsinterventies. Namelijk op het belang van de rol en identiteit van een reservist en het bijbehorende gedrag

[2] Voor de leesbaarheid is gekozen om Mechanisme of Action (MoA) uit de theorie vrij te vertalen naar beweegreden in de hoofdtekst van dit rapport. In bijlage 2 staat een uitleg van de gebruikte theorie en daarin wordt wel de technisch term MoA gebruikt

© Hogeschool Utrecht, 2026

ongeacht de context of setting. Ook hier kan het twee kanten op werken. Namelijk het vertonen van het 'juiste' gedrag omdat dit past bij de voorbeeldfunctie die je hebt en het niet vertonen van 'onjuist' gedrag omdat dit niet past bij de rol/ functie/ identiteit.
Juist voor reservisten die functioneren in tenminste drie belangrijke contexten; privé, werk en Defensie is dit van groot belang. Hiermee lijkt een aanknopingspunt voor de continuïteit van digitaal gedrag in verschillende contexten te zijn gevonden.

Beweegredenen en bijbehorende Behavioural Change Techniques (BCT's)

Zoals verder toegelicht in Bijlage 3 Verantwoording, is voor het ontwerpen van een passende interventie, van belang om een koppeling te maken tussen beweegredenen en bijbehorende Behavioural Change Techniques (technieken die je kunt gebruiken om mensen te stimuleren tot hun gedrag te veranderen naar het gewenste gedrag). Dit kunnen onder andere werkvormen zijn die je kunt opnemen in een training. In tabel 1 hieronder is te zien welke beweegredenen en BCT's zijn gelinkt en of ze relevant worden geacht voor reservisten.

Tabel 1: Mechanisms of Action met Behavioural Change Techniques

BCT's → MoA's ↓	Feedback on outcome(s) of behaviour	Social Support (unspecified	Social support (practical	Instruction on how to perform behaviour	Information about antecedents	Information about health consequences	Salience of consequences Use methods specifically	Information about social and environmental consequences	Anticipated regret	Information about emotional consequences	Pros and cons	Comparative imagining of future outcomes	Non-specific reward	Verbal persuasion about capability	Focus on past succes
Knowledge	Ja	Misschien	Ja	Ja	Toekomst of indirect		Ja		Misschien	Misschien					
Social/Professional role & identity														Misschien	Ja
Beliefs about consequences						Misschien	Ja	Misschien	Misschien	Misschien	Ja	Misschien	Ja		
Perceived susceptibility/vulnerability							Ja								

Bij de beweegredenen *Sociale en professionele rol en identiteit* en *waargenomen kwetsbaarheid* zijn er slechts een of twee Behavioral Change Techniques met een bewezen verband. De BCT "Focus on past succes" linkt met de Sociale en professionele rol en identiteit. Salience of consequences heeft een bewezen link met waargenomen kwetsbaarheid.
De andere twee beweegredenen *kennis* en *overtuigingen over de gevolgen* hebben met meerdere BCT's een bewezen verband. Van de BCT's met een link lijken er meerdere aan te sluiten op het profiel van een reservist. Daarmee zijn ze waarschijnlijk te gebruiken zijn om gedragsverandering bij reservisten te stimuleren. De BCT die het meest in het oog springt is **salience of consequences**, deze heeft een bewezen verband met drie van de vier beweegredenen. De **consequenties of gevolgen** van je eigen gedrag, voor jezelf of voor een ander wegen zwaar voor reservisten. Van de overige BCT's lijken een aantal relevant. Zoals **instructie** hoe je dient te handelen, **feedback** op de uitkomst van het handelen en **sociale support**. Ook het maken van een overzicht van de **voor- en nadelen**, aandacht voor eerder behaalde **successen** en wellicht een **beloning** zijn allemaal passend. Deze gedragsveranderingstechnieken zijn wetenschappelijk onderbouwd en passen bij de doelgroep.

Passende werkvormen zijn bijvoorbeeld:

© Hogeschool Utrecht, 2026

- Feedback over de gevolgen van bepaalde gedrag
  - Gebruik casussen waarin het mis is gegaan
- Refereer aan eerder succesvol toegepast gedrag
  - Gebruik succesvolle casussen
  - Laat zelf een lijst opstellen van digitaal veilig gedrag dat al wél wordt vertoond
- Leg de nadruk op de consequenties van het vertoonde gedrag (bijvoorbeeld met een relateerbare casus)
  - Consequentie van correct gedrag
  - Consequenties van incorrect gedrag (waar is het mis gegaan? En wat waren de gevolgen voor de persoon zelf, collega's, de organisatie en naasten)
- Instructie hoe te handelen
  - Oefen/ train ook dit handelen (bijvoorbeeld wat te doen bij een phishingmail)
  - Geef feedback op het handelen (wat ging goed, wat kan anders, waar zit de progressie)
- Bespreek hoe men elkaar kan steunen in het uitdragen en uitvoeren van veilig digitaal gedrag.
  - Wat is de norm die je met elkaar afspreekt
  - Spreek je elkaar aan?
  - Bespreek je de uitdagingen waar je tegenaan loopt
    - Hoe stel je een veilig wachtwoord in?
    - Hoe ga je om met geen contact met het thuisfront?
- Opstellen van een lijst met voor- en nadelen van het (in)correcte digitale gedrag
  - Wat levert het je op het (in)correct gedrag
  - Wat kost het (in)correct gedrag nu en in de mogelijke toekomst
- Belonen van correct gedrag

Een les die niet direct aan de gebuikte theorie te koppelen is, maar wel zeer relevant, is dat een reservist wel in staat moet zijn om gewenst gedrag te vertonen. In de morele beraden en het interview met commandanten kwam naar voren dat er een **gebrek is aan middelen** voor reservisten. Op het moment dat bepaalde communicatie alleen via een Defensie telefoon mag maar de reservist heeft die (nog) niet, dan is het onmogelijk om je aan de regels te houden.

Juridische grenzen

De geleerde lessen uit het juridische onderzoek zijn vastgelegd in 2 visuals met een uitleg erbij. De eerste is bedoeld voor beleidsmakers binnen Defensie en de tweede voor reservisten, zie verderop in dit rapport.

1) Er kan geconcludeerd worden dat Defensie op grond van de jurisprudentie wel degelijk beperkingen mag opleggen aan het gedrag van reservisten in het privéleven en bij de civiele baan, mits er een direct of indirect causaal verband bestaat met de veiligheid, integriteit of reputatie van Defensie.
De bevoegdheid om in te grijpen is echter niet onbegrensd. De rechter dwingt Defensie tot het hanteren van een strikte proportionaliteitstoets. Elke rechtspositionele maatregel moet aantoonbaar evenredig zijn aan de ernst van de gedraging en zijn gebaseerd op een zorgvuldige belangenafweging waarbij het beginsel van goed werkgeverschap te allen tijde wordt gerespecteerd. Daarnaast moet er ook aan de criteria van het Bărbulescu-arrest worden gehouden. Dit

© Hogeschool Utrecht, 2026

betekent dat naarmate het risico voor de veiligheid of de integriteit van Defensie concreter is, de ruimte voor de reservist om zich op zijn grondrechten te beroepen, evenredig afneemt.

2) De huidige maatregelen van Defensie om het digitale gedrag van reservisten in hun privétijd en bij hun civiele werkgever te reguleren komen vooral uit **interne richtlijnen**, namelijk de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag. De Gedragscode Defensie, de Gedragsregels Sociale Veiligheid & Integriteit Defensie en het Handboek Cyberveilig gedrag Defensie schrijven duidelijke normen en regels voor over digitaal gedrag binnen Defensieterrein en het digitaal gedrag in de privésfeer. Echter, **alleen de regels in de Gedragscode Defensie en de Gedragsregels Sociale Veiligheid & Integriteit Defensie zijn juridisch afdwingbaa**r, omdat er ook sancties in staan als deze regels worden overtreden.

3) Het Handboek Cyberveilig gedrag Defensie, de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit voldoen niet aan de eisen van artikel 135 van het Wetboek van Militair Strafrecht. Hierdoor vallen ze formeel gezien niet onder een dienstvoorschrift. Deze richtlijnen kennen een dualistisch karakter dat strikt afhankelijk is van de formele status van het document én de actuele status van de reservist.
Toch bepalen deze richtlijnen in zekere mate welke plichten reservisten hebben. Door de wettelijke status van reservisten als militair ambtenaar strekken deze plichten zich rechtmatig uit tot hun privéleven en hun civiele baan, mits hun digitale gedrag een directe impact heeft op de operationele veiligheid of de reputatie van Defensie. Reservisten horen zich namelijk als een goed militair ambtenaar te gedragen, ongeacht of ze op Defensieterrein of in de privésfeer of bij de civiele werkgever zijn. Dit staat ook in de Gedragscode waarvoor zij een eed of belofte hebben afgelegd.

4) Defensie kan een reservist alleen vervolgen op grond van het Wetboek van Militair Strafrecht, wanneer het digitale gedrag van de reservist in zijn privétijd of bij de civiele werkgever de operationele veiligheid van Defensie schaadt, een bedreiging vormt voor de veiligheid van de staat of de militaire orde. Als dit gedrag zowel onder het Wetboek van Militair Strafrecht als onder de Wet militair tuchtrecht valt, dan is in beginsel de commandant niet bevoegd om tuchtrechtelijk op te treden. Deze bevoegdheid ligt bij de strafrechter met uitzondering van de artikelen 6 tot en met 40 van de Wet militair tuchtrecht.

5) Als het gaat om controle of monitoring van het digitaal gedrag dan zijn de Bărbulescu arresten relevant.[3] Het Europees Hof voor de Rechten van de Mens (EHRM) heeft in de arresten Bărbulescu 2017 en de Nederlandse uitwerking daarvan, Hof Arnhem-Leeuwarden 2022, strikte criteria opgesteld voor de monitoring van digitaal gedrag in werkgever werknemer relatie:[4]

1. Voorafgaande informatie: Is de werknemer duidelijk geïnformeerd over monitoring?
2. Legitieme grond: Is er een zwaarwegend (veiligheids)belang?
3. Proportionaliteit en subsidiariteit: Kan het doel niet met minder ingrijpende middelen worden bereikt? Is de inbreuk in verhouding tot het risico?
4. Adequate waarborgen: Is er bescherming tegen misbruik van de gegevens?

Bij het toepassen van deze criteria op reservisten, ontstaat er een frictie tussen beleid en de evenredigheid.[5] Een reservist brengt het grootste deel van zijn tijd door in de civiele maatschappij en actieve controle door Defensie op zijn privéapparatuur, privéwachtwoorden of internetgedrag thuis vormt een disproportionele inbreuk op artikel 10 van de Grondwet, namelijk het recht

[3] Tijdschriftschrift Computerrecht 2022.
[4] EHRM 5 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608.
[5] Peters 2021.

© Hogeschool Utrecht, 2026

op eerbiediging van de persoonlijke levenssfeer.[6] Er is in de privésfeer geen sprake van een sluitend Defensienetwerk waar monitoring automatisch is toegestaan.[7] Een dwingende controlecultuur in de privésfeer of bij de civiele werkgever schendt het criterium subsidiariteit, als het doel ook via minder ingrijpende middelen kan worden bereikt.
Als het gaat om digitaal gedrag **binnen** het Defensie netwerk en Defensie locatie dan zou dit waarschijnlijk wel aan de criteria voldoen.

Ethische grenzen en resultaten van de morele beraden

1) In de drie morele beraden werd steeds geconcludeerd dat zelfs als je zelf niet op social media aangeeft dat je reservist bent dat mensen daar dan toch wel achter kunnen komen. Je buren zien je in uniform regelmatig het huis verlaten, vanuit je Google maps kan afgeleid worden dat je regelmatig naar een kazerne fietst of rijdt. Sommigen zagen bij aanvang van het moreel beraad geen risico's in de casussen (zolang ze niet weten dat ik bij Defensie werk maakt het niet uit) maar raakten tijdens het moreel beraad er wel van overtuigd dat het vrij makkelijk te achterhalen is dat ze reservist zijn. Dit maakt dat als er meer gegevens over je bekend zijn dat jij of je naasten een risico loopt om te worden lastiggevallen.

2) Ook geven reservisten aan dat er regels zijn over digitaal gedrag (bijv. niet in uniform op tinder). Deze regels zijn niet altijd duidelijk of consistent: zo waren er reservisten die op uitzending hun eigen laptop mee mochten hebben voor hun eigen bedrijf terwijl reservisten van andere eenheden dit niet mochten. Bovendien hebben reservisten niet altijd de middelen om de regels te volgen; zo had een van de reservisten nog geen Defensie telefoon en een Defensie laptop schijn je als reservist bijna nooit te krijgen.

3) Reservisten gaven in de morele beraden aan dat slordig digitaal gedrag zoals het hergebruik van wachtwoorden of het laten taggen in Strava iets zegt over het karakter van de persoon. Als je hier slordig mee omgaat privé, ben je dan bij Defensie ook lichtzinnig in het gebruik van digitale middelen? Dat leidt dan tot risico's voor Defensie.

4) Het verbieden van apps of het verplichten van unieke wachtwoorden heeft volgens reservisten alleen zin als het kunt controleren. Controleren van mobiele telefoons, privé agenda's of wachtwoorden is praktisch niet haalbaar en gaat veel van de reservisten ook te ver. Daaruit concluderen de reservisten dat verbieden en verplichten niet wenselijk is. Alleen bij specifieke gevoelige functies of een hoge alert state zouden er meer verboden en verplichtingen mogen zijn. Net zoals nu al geldt bij inzet tijdens crisissituaties of uitzendingen.

5) Reservisten verwachten veel van het verhogen van awareness (kennis en handelingsperspectief): als reservisten de risico's voor Defensie en hun eigen gezin inzien en weten wat ze moeten doen, dan veranderen ze hun digitaal gedrag. Uit het datalek bij Polarsteps blijkt wel dat het heel lastig is om door te hebben wat apps precies doen bijvoorbeeld met je locatie.

6) Reservisten stellen veiligheid van Defensie en hun eigen gezin, over het algemeen, boven het gemak of hun individuele vrijheid. Het schuurt als het gaat om het digitale gedrag van gezinsleden. Dat reservisten zelf gekozen hebben voor een rol als reservist maar hun gezin niet, weegt zwaar voor reservisten. Ze hebben wel overlegd met hun gezin maar zij hebben zelf gekozen om ook de risico's en eventuele beperkingen van het zijn van reservist te accepteren, hun gezin niet.

[6] De laat 2019.
[7] Damen & Baijens 2022.

© Hogeschool Utrecht, 2026

Aanbevelingen

Uit dit onderzoek volgen onderstaande aanbevelingen:

1) Reservisten hebben soms niet de middelen om het gewenste digitale gedrag te laten zien. Op het moment dat reservisten de middelen (nog) niet hebben dan heeft een training waarin uitgelegd wordt welk digitaal gedrag verwacht wordt geen zin.
2) De veelbelovende Behavioral Change Techniques kunnen deels als een onderdeel of oefening opgenomen worden in een training opgenomen, maar het gaat ook om doorlopende technieken. Een training af en toe is waarschijnlijk minder effectief dan een training gecombineerd met de doorlopende technieken, zie visual in Bijlage 1.
3) Controle van verplichtingen zien reservisten als erg belangrijk. Uit het juridische onderzoek volgt dat controle van digitaal gedrag tot op zeker hoogte en in specifieke situaties mogelijk is. Zorg dat dit verder onderzocht wordt. Uit het juridisch onderzoek hier blijkt dat dit kan als er een zwaarwegend veiligheidsbelang is (bijv. op missie of op Defensielocaties). Reservisten moeten dan vooraf over monitoring geïnformeerd zijn. De monitoring moet voldoen aan proportionaliteit en subsidiariteit: als het monitoren van enkel het feit dat er privé devices op een locatie aanwezig en digitaal zichtbaar zijn voldoende is, dan is binnendringen in devices niet proportioneel. Dit zou bijvoorbeeld kunnen betekenen dat als er een verbod is op het gebruik van privé devices, er een scan van het netwerk gemaakt kan worden. Aan een groep kan dan teruggekoppeld worden: er lijken x devices in dit netwerk te zijn die er niet mogen te zijn. Hoewel je in dit geval niet in devices binnendringt, is een procedure voor eventuele bijvangst wel nodig.
4) Er wordt gewerkt aan de rechtspositie van reservisten. Op dit moment wordt hier gekeken naar het arbeids- en het sociale zekerheidsrecht (ministerie van Arbeid en participatie en ministerie van Defensie, 2026). Het zou goed zijn om te onderzoeken of digitaal gedrag opgenomen kan worden hierin.

© Hogeschool Utrecht, 2026

Aandachtspunten en vervolg

Omdat het een klein project is van maar een jaar en het werven van reservisten lastig bleek, zijn de aantallen mensen die we gesproken hebben beperkt. Voor aanvang van het project hadden we gehoopt dat we via het reservisten bureau van Defensie reservisten zouden kunnen werven. Dit was niet mogelijk waardoor in de verschillende onderdelen Points of Contacts gezocht moesten worden en die Points of Contact zochten dan weer contact met reservisten. In de morele beraden hebben in totaal 20 reservisten meegedaan verdeeld over Landmacht, Luchtmacht en Marine. In totaal zijn er een kleine 10.000 reservisten bij Defensie waarvan de meesten bij de Landmacht en daarna de Marine en Luchtmacht. We hebben geen reservisten van de Marechaussee en de Bestuursstaf kunnen ontvangen in onze morele beraden, nu zijn de aantallen reservisten in die onderdelen ook laag.

Om ondanks de beperkte steekproef onder de reservisten te zorgen voor een gebalanceerd beeld, is voor de analyse van de beweegredenen gekozen om het vraagstuk vanuit verschillende perspectieven te bekijken: moreel beraad (3x, 20 reservisten in totaal), gedragsexpertise (interview), trainingsperspectief (interview), operationeel – commandanten reservisten (groepsinterview) en recruteringsprofiel (vacatures). Voor het juridische onderzoek is één interview gehouden.

Een specifiek groep reservisten, cyber reservisten, is expliciet niet meegenomen in deze analyse. Deze groep is expert in het onderwerp digitale veiligheid en is hier dagelijks, zowel voor Defensie als in hun civiele baan, mee bezig. Er kan dan ook verondersteld worden dat het digitaal gedrag en bewustzijn onder deze groep hoog is, en niet representatief voor de rest van de reservisten. Wel kan deze groep een rol spelen in een vervolgtraject waar ze een voorbeeldfunctie kunnen vervullen naar de andere reservisten en/of als trainer kunnen fungeren.

Met het in werking treden van de Cyberbeveiligingswet (Cbw) op 15 aug jl., zijn meer organisaties wettelijk verplicht om governance voor cyberveiligheid te verbeteren, hebben een zorgplicht (risicoanalyses maken en minimale maatregelen te nemen om cyberveiligheid te borgen) en een meldplicht hebben om incidenten te melden. Dit betekent waarshijnlijk dat meer reservisten in hun civiele baan te maken krijgen met de eisen vanuit de Cbw. Dit zou kunnen betekenen dat meer reservisten vanuit hun civiele baan al een hoger bewustzijn krijgen voor digitale risico's.

Verder onderzoek en ontwikkeling

Privé digitaal gedrag van medewerkers heeft een invloed op de digitale veiligheid van organisaties. Dit geldt voor alle organisaties maar de risico's voor medewerkers en organisaties in het veiligheidsveld zijn waarschijnlijk groter dan voor andere organisatie. Dit wordt steeds belangrijker omdat het voor medewerkers steeds lastiger wordt om privé ook veilig digitaal gedrag te hebben.

Uit de morele beraden blijkt dat voor verplichtingen of verboden reservisten het belangrijk vinden om die verplichtingen en verboden dan ook te kunnen controleren. Als er niet gecontroleerd kan worden dan heeft een verplichting volgens reservisten niet zoveel zin. De criteria die het Hof Arnhem-Leeuwarden op basis van de Bărbulescu arresten geformuleerd hebben lijken monitoring in de privésfeer en bij de civiele baan niet toe te staan, maar op Defensielocaties wel. De mogelijkheid om digitaal gedrag te kunnen monitoren moeten verder uitgezocht worden.

Op basis van de hier aangewezen Behavioral Change Techniques zouden de trainingen digitale veiligheid van Defensie aangepast kunnen worden. Als je een daadwerkelijk effect wilt kunnen meten dan moet je onder een representatieve groep reservisten voor het aanpassen van de training hun awareness meten en na het invoeren van vernieuwde trainingen. Of je moet nieuwe reservisten in twee groepen verdelen en de ene de nu bestaande trainingen geven en de

© Hogeschool Utrecht, 2026

andere de vernieuwde. Dit zou erg interessant onderzoek zijn, maar ook een groot project waar vooraf de medewerking van heel Defensie geregeld moet zijn.

Naast de vier besproken beweegredenen is er een groep van vier andere die minder overtuigend naar voren komen uit de huidige analyse, maar wellicht interessant zijn voor verder onderzoek. Dit zijn:

- (Sociale) normen ((*Social) norms*)
    - De houding en het gedrag van andere mensen binnen een sociale groep. De eigen perceptie van wat de meeste andere mensen binnen een sociale groep geloven en doen.
- Waarden (*Values)*
    - Morele, sociale of esthetische principes die door een individu of een samenleving worden aanvaard als leidraad voor wat goed, wenselijk of belangrijk is.
- Motivatie (*Motivation*)
    - Processen die verband houden met de drijfveer die gedrag een doel of richting geeft en die op bewust of onbewust niveau plaatsvinden.
- Omgevingscontext en hulpbronnen (*Environmental context & resources)*
    - Aspecten van iemands situatie of omgeving die het gedrag ontmoedigen of juist stimuleren.

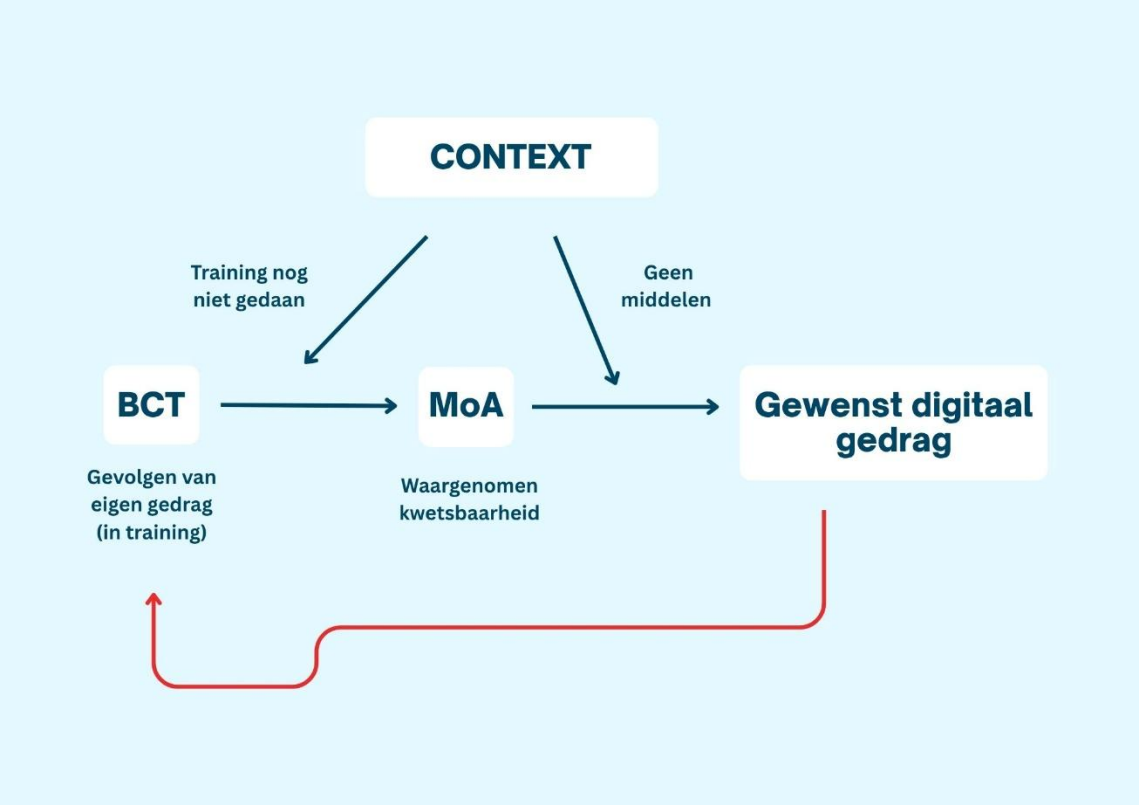
Zoals in de inleiding al vermeld zijn reservisten van Defensie slechts een deel van de mensen die naast hun privé leven en een baan ook nog als reservist of vrijwilliger ingeschakeld kunnen worden bij organisaties in het veiligheidsveld en sinds Covid ook in de zorg. Het zou interessant zijn om dit onderzoek uit te breiden naar vrijwilligers bij de politie en brandweer. Het zou ook interessant zijn om uit te zoeken wat de beweegredenen en Behavioral Change Techniques zijn die passen bij deze vrijwilligers. In morele beraden zou dan bekeken kunnen worden waar politie vrijwilligers en brandweer vrijwilligers een ethische grens trekken. Ook de juridische grenzen zouden dan weer bekeken moeten worden.

Militair civiele samenwerking zou een interessante context zijn voor verder onderzoek: dan heb je zowel militaire als civiele organisaties met ieder hun eigen regels op het gebied van digitaal gedrag en mogelijkheden die moeten samenwerken. Hebben ze dan allemaal dezelfde mogelijkheden, middelen en kennis voor veilig communiceren? Hoe wordt dat dan gedaan en past dat dan binnen de regels en afspraken van de eigen organisatie?

© Hogeschool Utrecht, 2026

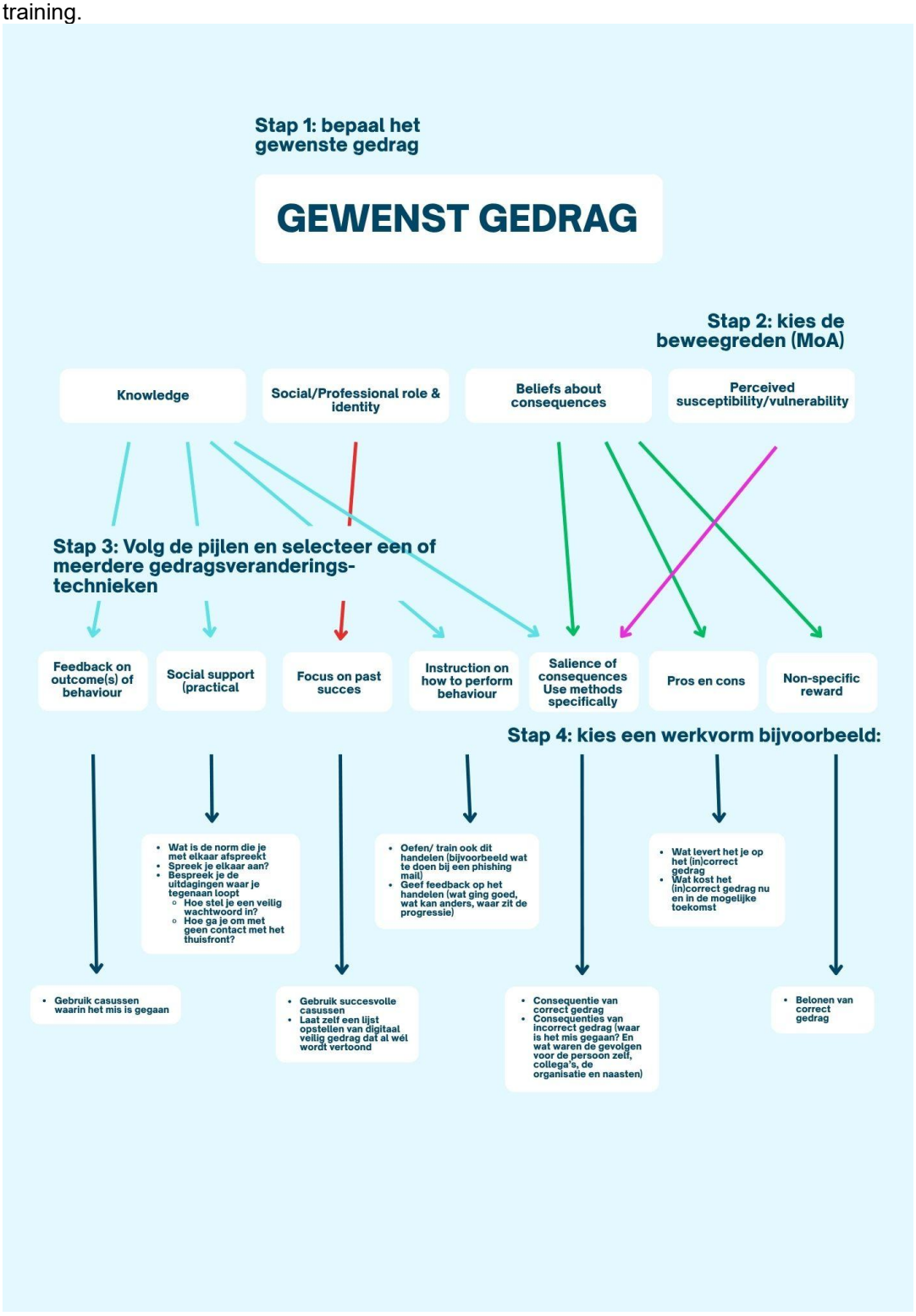
Bijlage 1 Visuals

Voorbeeld relatie Behavioral Change Technique, context en beweegreden (Mechanism of Action)

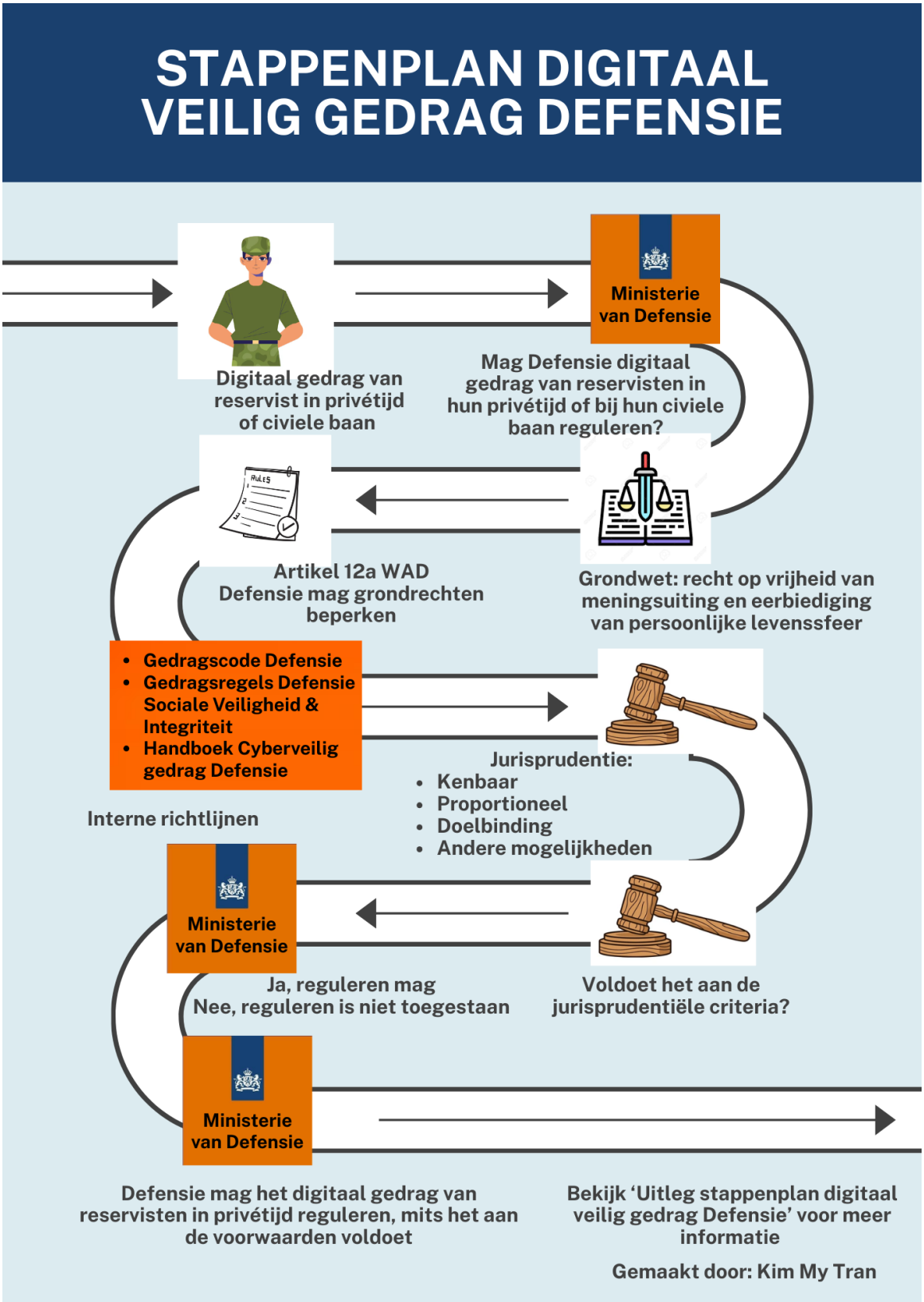


© Hogeschool Utrecht, 2026

Van gewenst gedrag via beweegredenen naar voorbeelden van passende werkvormen in een training.



© Hogeschool Utrecht, 2026



© Hogeschool Utrecht, 2026

UITLEG STAPPENPLAN DIGITAAL VEILIG GEDRAG DEFENSIE

Hieronder worden de stappen van het stappenplan toegelicht.

Digitaal gedrag van reservist in privétijd en bij civiele baan
Reservisten hebben een directe en grote invloed op de veiligheid van Defensie. Zij bewegen zich voortdurend op het grensvlak tussen de civiele en de militaire wereld. Het digitale gedrag van een reservist vormt daarbij een belangrijke veiligheidsfactor voor Defensie. Hierbij kan worden gedacht aan het hergebruiken van wachtwoorden voor zowel privé als Defensie of het gebruik van social media.

Mag Defensie het digitaal gedrag van reservisten in hun privétijd en bij hun civiele baan reguleren?
Ter waarborging van de veiligheid van Defensie kan het noodzakelijk zijn het digitale gedrag van reservisten in hun privétijd of bij hun civiele baan te reguleren. Hierbij is het van belang dat er aan bepaalde voorwaarden wordt voldaan.

Interne richtlijnen
De Gedragscode Defensie is nader uitgewerkt in de Gedragsregels Defensie Sociale Veiligheid & Integriteit. Hierin is vastgelegd wat van een defensiemedewerker wordt verwacht. Het overtreden van deze regels kan leiden tot aangifte of het opleggen van een andere sanctie. Dit is afhankelijk van de zwaarte van de overtreding. Daarnaast bevat het Handboek Cyberveilig Gedrag Defensie richtlijnen voor veilig digitaal gedrag.

Voorwaarden
Reservisten hebben, net als ieder andere Nederlander, recht op vrijheid van meningsuiting en het recht op eerbiediging van de persoonlijke levenssfeer. Echter, deze rechten kunnen worden beperkt door Defensie op grond van de wetgeving.

Uit jurisprudentie zijn verschillende criteria naar voren gekomen voor het reguleren van het gedrag van een werknemer buiten werktijd.
- Voorafgaande informatie: Is de werknemer duidelijk geïnformeerd over monitoring?
- Legitieme grond: Is er een zwaarwegend (veiligheid)belang?
- Proportionaliteit en subsidiariteit: Kan het doel niet met minder ingrijpende middelen worden bereikt? Is de inbreuk in verhouding tot het risico?
- Adequate waarborgen: Is er bescherming tegen misbruik van de gegevens?

Conclusie
Defensie mag het digitaal gedrag van reservisten in hun privétijd of bij hun civiele baan reguleren, mits er aan de voorwaarden wordt voldaan.

Wetgeving: artikel 7 en 10 Grondwet, artikel 12a Wet ambtenaren defensie
Jurisprudentie: Bărbulescu ECLI:CE:ECHR:2017:0905JUD006149608.

Gemaakt door: Kim My Tran

© Hogeschool Utrecht, 2026

STAPPENPLAN DIGITAAL GEDRAG ALS RESERVIST



Thuis + Werk + Defensie

Voorbeelden van minder veilig gedrag:

- Socialemediagebruik:
  - Voorbeeld: Strava op mobiel
- Wachtwoorden hergebruiken (of simpele wachtwoorden)
- Locatie delen
  - Social media apps
  - Google Maps
- Wifi router thuis (wifi delen met anderen)
  - Vrienden
  - Kennissen

→ Ministerie van Defensie

Veiligheid van Defensie

→ 

Veiligheid van thuis

Gevaren:



- Datalekken
- Hacks
- Achterhalen privégegevens uzelf en uw gezinsleden
- Doxing (thuis)
- Via internet lastig gevallen worden

Wat zijn de regels?

- Gedragscode Defensie
  - Verbondenheid
  - Veiligheid
  - Vertrouwen
  - Verantwoordelijkheid
- Gedragsregels Defensie Sociale Veiligheid & Integriteit

→ Gebruik het Handboek Cyberveilig gedrag Defensie. De tips die hierin staan zijn deels ook waardevol voor thuis en civiele baan





Thuis Werk

Gemaakt door: Kim My Tran

© Hogeschool Utrecht, 2026

UITLEG DIGITAAL GEDRAG ALS RESERVIST

Waarom is het belangrijk?
Het digitaal gedrag van een reservist in de privétijd en bij de civiele baan heeft invloed op de veiligheid van Defensie. Daarnaast kan het ook zijn dat de veiligheid van de reservist en zijn thuisfront geschaad worden. Een voorbeeld hiervan is het gebruik van Strava. Door het gebruik van Strava zijn privégegevens zoals naam en adres van militairen gelekt. Onveilig digitaal gedrag kan leiden tot doxing.

Doxing is kortweg het met kwade bedoelingen verzamelen of (verder) verspreiden van persoonlijke, gevoelige of privéinformatie zoals woonadres, telefoonnummer, een foto, paspoort, naam werkgever en gegevens van familie of combinaties. Kortom, persoonsgegevens zijn alle gegevens waarmee een persoon te identificeren is.

Interne richtlijnen
Voor specifieke gedragsregels en tips kunnen reservisten de interne richtlijnen bekijken:

- De Gedragsregels Defensie Sociale Veiligheid & Integriteit
  - Ik ben bewust van de risico's van het gebruik van social media. (pagina 10)
  - Ik ga zorgvuldig om met mijn diensttelefoon. (pagina 14)
  - Ik maak verantwoord gebruik van Defensie-internet en e-mail. (pagina 14)
  - Ik bespreek mijn nevenwerk. (pagina 19)
  - Ik voer geen verboden nevenwerk uit. (pagina 20)
  - Ik voorkom (iedere schijn van) belangenverstrengeling. (pagina 22)
  - Ik gebruik informatie alleen voor de uitoefening van mijn functie. (pagina 25)
- Het Handboek Cyberveilig gedrag Defensie

Er staan hier gedragsregels en tips in die waardevol zijn voor het digitaal gedrag van een reservist bij Defensie, als thuis en bij de civiele baan.

Het volgen van de gedragsregels is belangrijk voor de veiligheid van de reservist en van Defensie.

Gemaakt door: Kim My Tran

© Hogeschool Utrecht, 2026

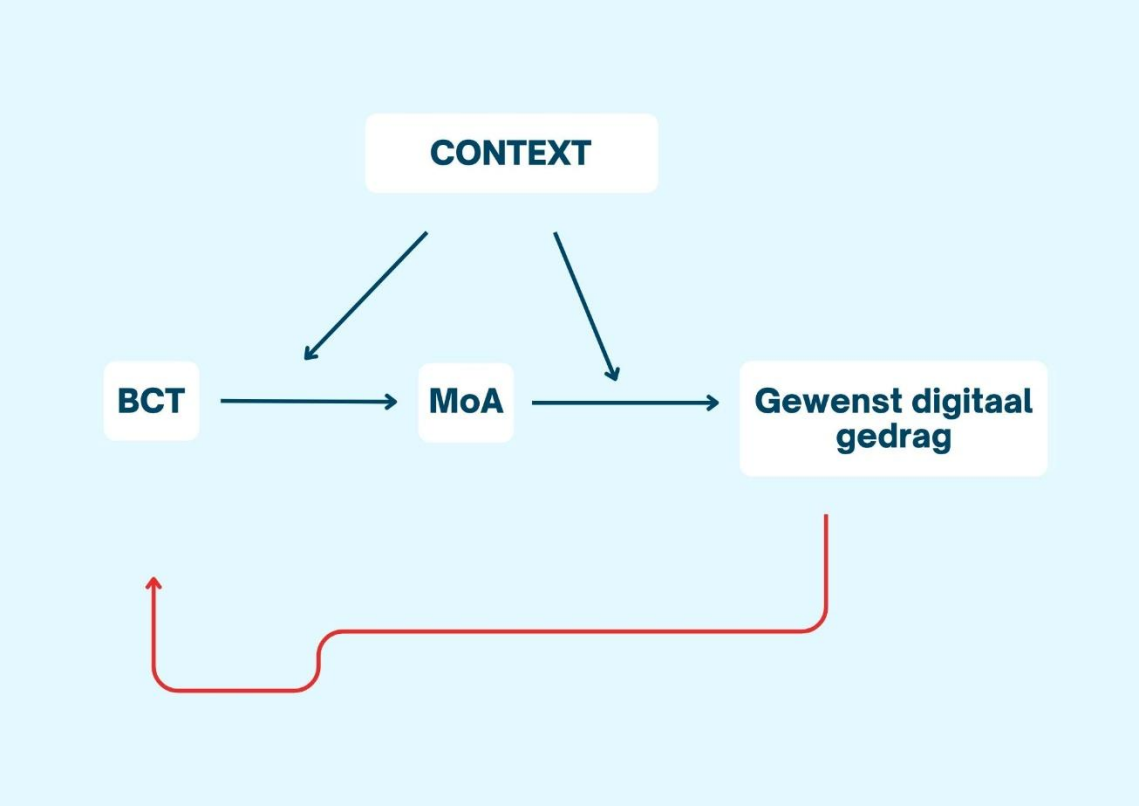
Bijlage 2 Mechanisms of Action en Behavioral Change Techniques

De hoofdvraag van dit onderzoek luidt:

Hoe kunnen we voorkomen dat het digitaal gedrag van reservisten in de privésfeer en de andere betrekkingen tot risico's voor Defensie leidt, rekening houdend met individuele rechten en ethiek?

Gedrag en daarmee ook digitaal gedrag kan natuurlijk nooit volledig beheerst worden. Wat wél mogelijk is, is het beïnvloeden van gedrag in gewenste richting. Het beïnvloeden van gedrag middels nudging, sociale beïnvloeding of andere gedragsbeïnvloedingsmechanismen is een bekende en beproefde techniek die in vele sectoren wordt gebruikt.

Om de hoofdvraag van dit onderzoek te kunnen beantwoorden wordt gebruik gemaakt van onderstaand model vrij naar Schenk et.al. (afbeelding 1). Waarbij de gedragsinterventie (*intervention*), actiemechanisme (*Mechanisms of Action* (MoA's) en doelgedrag (*outcome behaviour*) de focus hebben. Voor de leesbaarheid hebben we in de hoofdtekst Mechanismes of Action vrij vertaald naar beweegreden. In de bijlages kiezen we ervoor de technische term Mechanism of Action te gebruiken.



Figuur 1: Model Behavioural Change Techniques, Mechanisms of Action en gedrag

© Hogeschool Utrecht, 2026

In dit onderzoek is eerste instantie gekeken naar de *contex*t factoren. Het gaat om het spanningsveld tussen privé, werk en werk voor Defensie. Militairen en dan specifieker reservisten zijn de populatie.
Deze contextfactoren grijpen in op het werkende mechanisme (MoA) dat het doelgedrag kan veranderen. Vandaar dat deze MoA's centraal staan in het onderzoek en de analyse. Wanneer de MoA's bekend zijn, kan worden terug geredeneerd welke gedragsveranderingstechniek (Behavioral Change Technique (BCT)) ingezet kan worden. Een BCT is een interventie (*Intervention*). Hiervoor is gewerkt met de Theory & Techniques'-tool (TaTT) (https://theoryandtechniquetool.humanbehaviourchange.org/)van het *Human Behaviour Change Project*.

Wat is de 'Theory & Techniques'-tool?

Deze tool is onderdeel van *het Human Behaviour Change Project* een samenwerkingsverband tussen toonaangevende instellingen wereldwijd dat tot doel heeft een systeem te ontwikkelen waarmee bewijsmateriaal over interventies gericht op gedragsverandering kan worden samengevat, geïnterpreteerd en verspreid, zie onder andere (Carey et al., 2019).

De '*Theory & Techniques'*-tool (https://theoryandtechniquetool.humanbehaviourchange.org/) is een heatmap van 74 BCT's en 26 overkoepelende MoA's, wat resulteert in 1924 cellen. Elke cel vertegenwoordigt het verband tussen een BCT en een MoA, waarbij sterkere verbanden in het groen worden weergegeven. De sterkte van een verband wordt bepaald door een synthese van de wetenschappelijke literatuur en een consensusonderzoek onder deskundigen. Binnen elke BCT-MoA-cel zijn de resultaten te vinden van de literatuurstudie, de consensusstudie en de triangulatie. Door op een cel te klikken, zie je een verwijzing naar alle studies die gebruikt zijn om de cel in te vullen.
Bij de analyse is gewerkt met een lijst van 25 van de 26 MOA's uit de oorspronkelijke tool. Er is gekozen om Norms en Social Norms samen te voegen vanwege beperkt onderscheidend karakter. Zie tabel 2 hieronder voor de volledige lijst van MoA's met definitie.

Tabel 2: Lijst Mechanisms of Action met definitie

MoA	Definitie
Social/Professional role & identity	A coherent set of behaviours and displayed personal qualities of an individual in a social or work setting.
Perceived susceptibility/vulnerability	Perceptions of the likelihood that one is vulnerable to a threat.
Beliefs about consequences	Beliefs about the consequences of a behaviour (i.e. perceptions about what will be achieved and/or lost by undertaking a behaviour, as well as the probability that it will lead to a specific outcome).
Knowledge	An awareness of the existence of something.
(Social) Norms	The attitudes held and behaviours exhibited by other people within a social group. One's perceptions of what most other people within a social group believe and do.
Values	Moral, social or aesthetic principles accepted by an individual or society as a guide to what is good, desirable or important.
Motivation	Processes relating to the impetus that gives purpose or direction to behaviour and operates at a conscious or unconscious level.
Environmental context & resources	Aspects of a person's situation or environment that discourage or encourage the behaviour.
Skill	An ability or proficiency acquired through practice.

© Hogeschool Utrecht, 2026

Social influence	Those interpersonal processes that can cause oneself to change one's thoughts, feelings or behaviours
Reinforcement	Processes by which the frequency or probability of a response is increased through a dependent relationship or contingency with a stimulus or circumstance.
(vervolg) **MoA**	Definitie
Needs	Deficit of something required for survival, well-being or personal fulfilment.
Emotion	A complex reaction pattern involving experiential, behavioural, and physiological elements.
Social learning	A process by which thoughts, feelings and motivational states observed in others are internalised and replicated without the need for conscious awareness.
General attitudes/beliefs	Evaluations of an object, person, group, issue or concept on a scale ranging from negative to positive.
Beliefs about capabilities	Beliefs about one's ability to successfully carry out a behaviour.
Optimism	Confidence that things will happen for the best or that desired goals will be attained.
Intention	A conscious decision to perform a behaviour or a resolve to act in a certain way.
Goals	Mental representations of outcomes or end states that an individual wants to achieve.
Memory, attention & decision processes	Ability to retain information, focus on aspects of the environment and choose between two or more alternatives.
Behavioural regulation	Behavioural, cognitive and/or emotional skills for managing or changing behaviour.
Attitude towards the behaviour	The general evaluations of the behaviour on a scale ranging from negative to positive.
Self-image	One's conception and evaluation of oneself, including psychological and physical characteristics, qualities and skills.
Behavioural cueing	Processes by which behaviour is triggered from either the external environment, the performance of another behaviour, or from ideas appearing in consciousness.

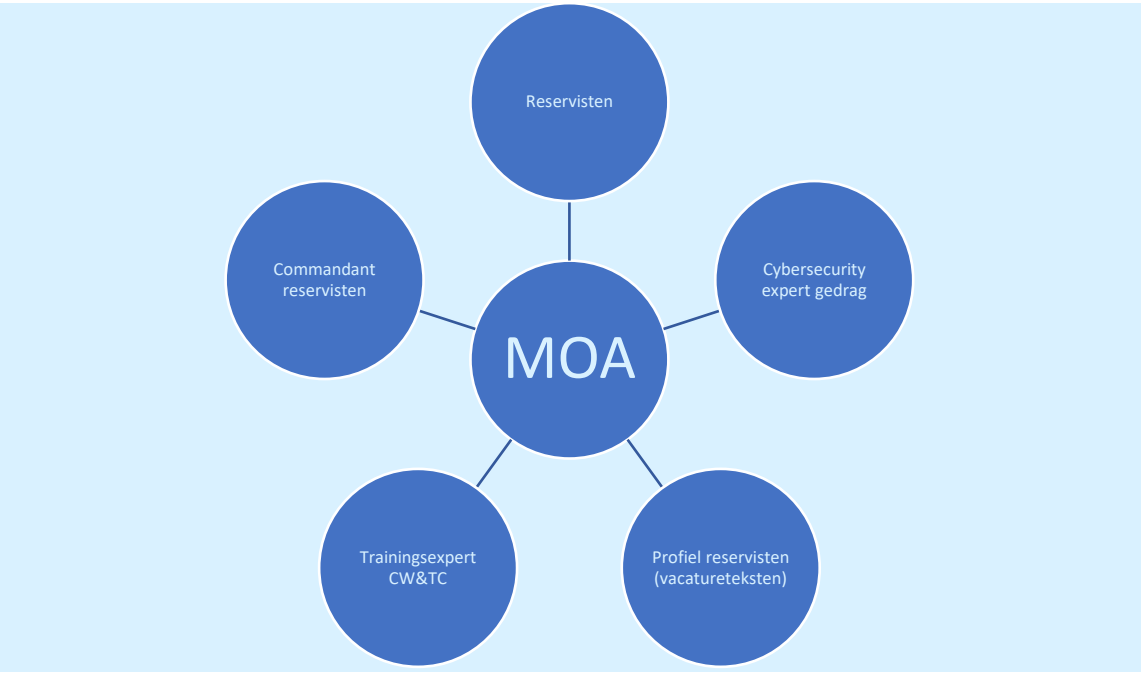
© Hogeschool Utrecht, 2026

Bijlage 3 Verantwoording

Inleiding onderzoeksmethode en type bronnen

Dit onderzoek naar digitaal veilig gedrag bij reservisten van Defensie is een eerste verkenning naar mogelijke aanknopingspunten voor gedragsverandering. Omdat het een eerste verkenning is, is gekozen om vanuit zoveel mogelijk perspectieven naar dit vraagstuk te kijken. De nadruk ligt dan ook op de variëteit in bronnen en niet zozeer de kwantiteit. Zo zijn er interviews afgenomen met commandanten van reservisten, een cybersecurity expert op het gebied van gedrag en een interview met een trainingsexpert van het CWTC. Ook hebben er een drietal moreel beraden plaatsgevonden met reservisten. Verder zijn de vacaturetesten voor reservisten geanalyseerd.

Met andere woorden, de perspectieven van de reservist, de commandanten van reservisten, trainingsexpert, gedragsexpert en het vacatureprofiel zijn aanwezig.



Figuur 2: de in dit onderzoek meegenomen perspectieven

Hieronder is een uitgebreide beschrijving te vinden per type bron.

Profiel Reservisten: Vacatureteksten

De analyse van de vacatureteksten heeft in twee stappen plaatsgevonden. In week 45 en 46 van 2025 zijn alle vacatureteksten voor reservisten op de website van Defensie bekeken en geanalyseerd. De vacatures voor reservisten omvatten zowel de vacatures voor ‘nieuwe’

© Hogeschool Utrecht, 2026

reservisten als voor ‘herintreders’, reservisten die eerder als militair in dienst zijn geweest bij Defensie. Op basis van alle vacatures is een standaardstructuur voor de vacatures gedestilleerd. De standaardstructuur met bijbehorende onderdelen kwamen in (zo goed als) iedere vacaturetekst in verschillende bewoordingen voor. Voor de analyse is voor al deze tekstonderdelen de meest generieke bewoording gekozen. De bijbehorende teksteenheden zijn opgenomen in de coderingstabel voor verdere analyse m.b.t. gedragskenmerken. Aanvullend zijn nog algemene definities en functiebeschrijvingen opgenomen. Zoals bijvoorbeeld de definitie en algemene functiebeschrijving van een reservist.

Interviews

Er zijn ook 4 (groeps-)interviews gehouden in dit project.
- met een cybersecurity expert op het gebied van gedrag
- een groepsinterview met drie commandanten van reservisten
- een Defensiemedewerker van Cyber Warfare & Training Centre (CWTC) (trainingsexpert)
- een Defensiemedewerker van de afdeling Beleid en Analyse bij het Kenniscentrum van de Centrale Organisatie Integriteit Defensie (COID) (niet meegenomen in de analyse voor gedrag wel in het juridisch onderzoek)

De interviews met de cybersecurity experts, de Defensie medewerker CWTC en de Defensiemedewerker COID zijn opgenomen en getranscribeerd. De interviews met de cybersecurity expert en de medewerker van het CWTC zijn na het transcriberen per teksteenheid gecodeerd. Het groepsinterview met de commandanten is niet opgenomen, maar hiervan is een gespreksverslag gemaakt. Dit gespreksverslag is per teksteenheid gecodeerd.

Reservisten: Morele beraden

Om de ethische grenzen van het beïnvloeden van digitaal gedrag van reservisten te verkennen is besloten om morele beraden te houden. Tijdens een moreel beraad bespreken betrokkenen een casus en welke waarden er spelen in die casus. Het is een methode waarin deelnemers gezamenlijk hun eigen waarden verkennen aan de hand van een casus en tot een consensus proberen te komen over wat goed zou zijn om te doen. De morele beraden kenden een socratische gespreksvorm waarin de reservisten aan de hand van de casus systematisch de volgende stappen doorliepen:

1. **Verkennen:** Situatieschets. Wat is er aan de hand? Wie zijn de betrokkenen? Welke handelingsopties zijn er?
2. **Ruimte voor verhelderingsvragen over de situatieschets:** zijn er dingen onduidelijk?
3. **Onderzoeken**: Wat is de ethische vraag? (*Is het goed dat…?*)
4. **Individuele standpunten:** Beargumenteer je standpunt vanuit waarden. (*Het is goed dat (…), want [waarde]. OF: het is niet goed dat (…), want [waarde].*)
5. **Vergelijken van de standpunten:** verschillen en overeenkomsten.
6. **Afwegen:** Welke standpunten hebben volgens de groep het meeste gewicht? Hoe wegen jullie deze tegen elkaar af? Wat is jullie antwoord op de ethische vraag?

Er zijn drie morele beraden gehouden. In elk moreel beraad werd een andere casus behandeld. De morele beraden werden begeleid door een ervaren begeleider die verder geen rol had in het project, dit om mogelijke beïnvloeding van het morele beraad door de begeleider te voorkomen. Voor het gebruik van de morele beraden in dit project is geïnformeerde toestemming gevraagd. Om te voorkomen dat namen van reservisten tien jaar moeten worden bewaard is het vragen van toestemming in verschillende stappen gegaan. Een contactpersoon van Defensie stuurde een aankondiging rond in het eigen Defensie onderdeel. Reservisten meldden zich aan bij deze contactpersoon. Voor aanvang van het morele beraad is de informatie nogmaals gegeven aan de reservisten en vervolgens zijn de onderzoekers uit de zaal gelopen zodat reservisten nog eventueel vragen zouden kunnen stellen aan de onafhankelijke begeleider en weg zouden

© Hogeschool Utrecht, 2026

kunnen gaan zonder door de onderzoekers gezien te worden. Daarna hebben reservisten een kruisje gezet op een toestemmingsformulier, zonder hun naam hierop te zetten. Deze werkwijze is voorgelegd aan de Ethische Commissie Onderzoek- kamer Sociaal Domein van de Hogeschool Utrecht en hierop volgde positief advies.
Moreel beraad 1 en 2 vonden plaats op vrijdag 13 feb 2026 tussen 15.30-17.00 uur 2026 in het HU gebouw in Amersfoort. Het derde morele beraad werd gehouden op vrijdag 29 mei van 15.30- 17.00 uur in een gebouw van de Bernhardkazerne in Amersfoort.

Bij casus 1 waren 5 reservisten van Luchtmacht en Marine aanwezig en werd onderstaande casus behandeld:

Casus 1: In je huishouden gebruiken jullie altijd hetzelfde wachtwoord, dus de Ring deurbel, de Nest thermostaat, Netflix, HBO, ESPN. Inlognaam is jouw achternaam en wachtwoord [straatnaam, huisnummer] (dus Kerkstraat2). Jullie hebben een tijd lang overal een ander wachtwoord voor gebruikt maar dan werd je steeds door je kinderen gebeld met de vraag "Wat het wachtwoord is voor thermostaat of Netflix?".

Bij casus 2 waren 6 reservisten van Luchtmacht en Marine aanwezig en werd deze casus behandeld:

Casus 2: In de groep waar je mee hardloopt houdt iedereen Strava bij. Er is een competitie waarbij groepsleden eerst gezamenlijk en daarna een aantal keer alleen hetzelfde rondje lopen. Je bent je sporthorloge vergeten en vraagt een ander je te taggen omdat je de route wilt bewaren. Degene die je tagt heeft een heel open Strava account en laat ook altijd zien met wie hij loopt.

Bij casus 3 waren 9 reservisten van het Korps nationale reserve aanwezig. Een van de reservisten was een officier.

Casus 3: Je hebt als reservist steeds drie agenda's die je op elkaar moet afstemmen. Het handigste is als je alle agenda's in een samenbrengt en die gesynchroniseerd houdt. Hiervoor exporteer je alle Defensie afspraken en de afspraken van je civiele baan naar je privé agenda. Zo heb je een agenda waarbij je altijd weet voor welke

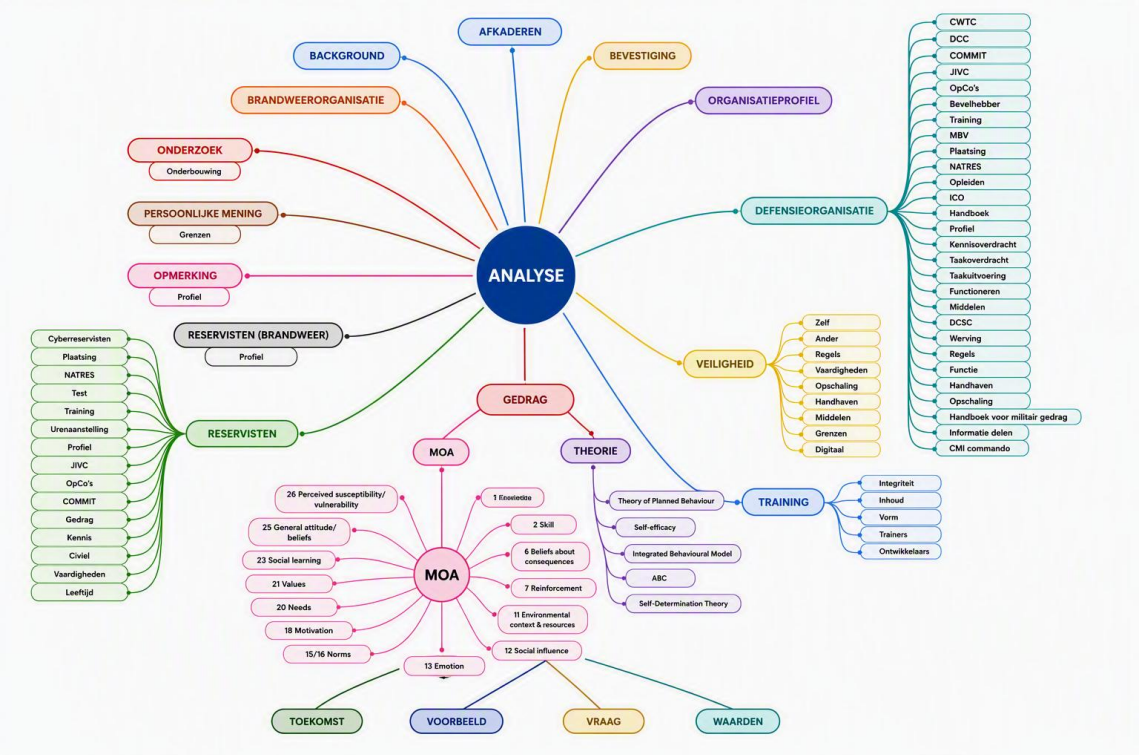
© Hogeschool Utrecht, 2026

afspraak, met wie je op welke locatie moet zijn. Omdat je dit in je privé agenda doet weet je partner dit ook.

Verslaglegging van de morele beraden is gedaan door bij elke moreel beraad een of twee onderzoekers aantekeningen te laten maken. Van de moreel beraden zijn gespreksverslagen gemaakt op basis van deze aantekeningen. Deze verslagen zijn ook per teksteenheid gecodeerd.

Analyse

Alle teksten: de transcripten en samenvattingen van de interviews en de gespreksverslagen van de moreel beraden zijn allemaal opgeknipt in kleine losstaande teksteenheden. Iedere teksteenheid is in eerste instantie gecodeerd op basis van de hoofdcategorieën. Indien er sprake was van een subcategorie, dan is deze ook gecodeerd. Zie figuur 3 hieronder voor het overzicht van de hoofd- en subcategorieën.



Figuur 3: hoofd- en subcategorieën inclusief de MoA's.

Daarnaast is er bij de hoofdcategorie gedrag gewerkt met een subcategorie MoA. Per teksteenheid is, waar van toepassing, een specifieke MoA toegekend. Deze MoA's zijn de basis voor de analyse, met als doel aanknopingspunten te vinden voor gedragsverandering.
Bij de analyse is gewerkt met een lijst van 25 MoA's uit de oorspronkelijke lijst van TaTT, zie de uitleg over Mechanismes of Action in Bijlage 2.

Voor de meest voorkomende MoA's in dit onderzoek is bekeken met welke Behavioural Change Technique (BCT) er een wetenschappelijk verband is aangetoond. Vervolgens is door twee

© Hogeschool Utrecht, 2026

onderzoekers bepaald of de BCT relevant kan zijn voor de doelgroep reservist en/ of de Defensieorganisatie. Dit is gedaan op basis van een beargumenteerde inschatting met behulp van de verzamelde informatie over het profiel van de reservist en de organisatie.

Resultaten

Profiel reservisten: Vacatureteksten

Ten tijde van de dataverzameling (week 45 en 46 van 2025) stonden er 46 vacatures voor reservisten online. Hieronder vielen vacatures voor zowel 'nieuwe' reservisten als 'herintreders' (reservisten die kort geleden als militair in dienst waren bij Defensie). In deze 46 vacatures zijn alle hoofdonderdelen van de krijgsmacht vertegenwoordigd. In Tabel 3 zijn de aantallen uitgesplitst per onderdeel te vinden. Opvallend is dat meer dan de helft van de vacatures voor reservisten bij de Landmacht zijn.

Tabel 3 : Reservistenvacatures uitgesplitst per onderdeel van de krijgsmacht.

Reservisten functies per onderdeel van de krijgsmacht (op 13 -11-2025)	**aantal**	**Functies**	**opleidingsniveau**
Marine	4	Reserve officier, reserve onderofficier, reserve manschap	VMBO tot WO
Landmacht	31	Divers	
Luchtmacht	6	Bewaken en beveiligen, chauffeur,	MBO tot WO
Marechaussee	4	Bewaken en beveiligen en grenswachter	VMBO, MBO HAVO
Bestuursstaf	1	Defensity college	
Defensity college (komt terug bij ieder onderdeel; na middelbare school VMBO en hoger)			

Na analyse is gebleken dat de vacatureteksten volgens eenzelfde structuur zijn opgebouwd. In het kader hieronder is de algemene structuur te vinden.

© Hogeschool Utrecht, 2026

Kader 1: Opbouw vacaturetekst reservistenfunctie

- Een korte beschrijving van de functie inclusief opleidingsniveau en leeftijdsgrenzen
- Wat verwacht wordt van de reservist
  - Verplichte trainingen/ oefeningen
  - Inzet
  - Voorbeeldfunctie
- Een schets van het gezochte profiel. Veel voorkomende profielwensen zijn;
  - Teamspeler,
  - Sportief,
- Redenen om reservist te worden
  - Gratis sporten (onder werktijd)
  - Zingeving
  - Vrijetijdsbesteding
  - Bijdrage aan de samenleving
  - Persoonlijke ontwikkeling

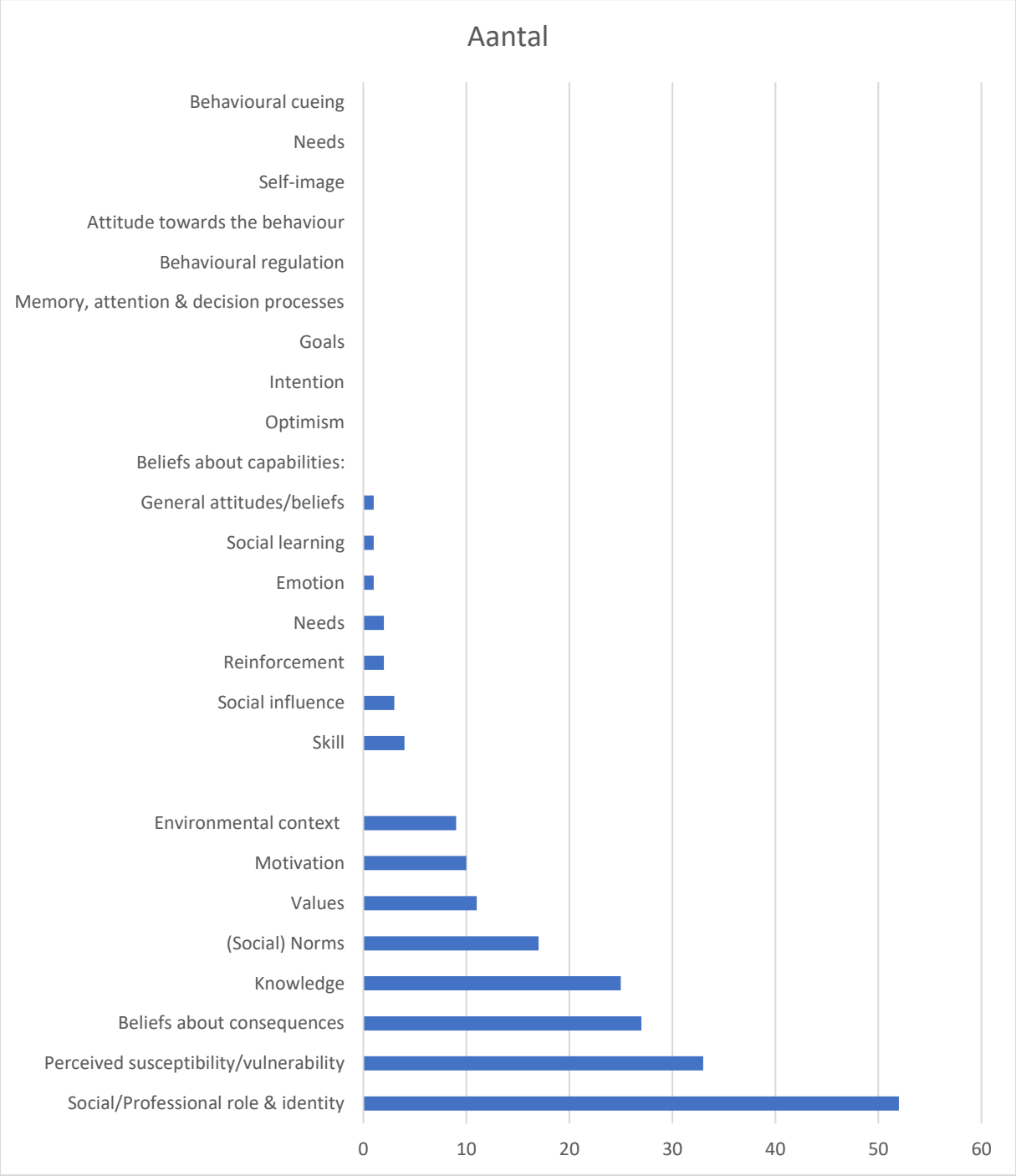
Bovenstaande onderdelen kwamen in (zo goed als) iedere vacaturetekst in verschillende bewoordingen naar aan bod. Voor de analyse is voor al deze tekstonderdelen de meest generieke bewoording gekozen. De bijbehorende teksteenheden zijn opgenomen in de coderingstabel voor verdere analyse. Aanvullend zijn nog algemene definities en functiebeschrijvingen opgenomen. Zoals bijvoorbeeld de definitie en algemene functiebeschrijving van een reservist. Van deze vacatures zijn dus niet de volledige teksten opgenomen in de analyse.
Bevindingen met betrekking tot het gedragsprofiel worden beschreven bij de analyse van de gedragskenmerken.

Analyse van de tekst fragmenten

Allereerst is bekeken of alle teksten (vactureteksten, interviewverslagen en verslagen van morele beraden) tekstfragmenten bevatten die inderdaad het label gedrag kregen. Dat was het geval. In de verslagen van de morele beraden kwam het label *gedrag* het meeste voor, in het verslag van het groepsinterview met commandanten het minste. Van de in totaal 1356 markeringen van teksteenheden uit alle teksten (vacatureteksten, interviewverslagen en verslagen van morele beraden) zijn 249 tekstonderdelen gemarkeerd onder de categorie *gedrag*. Van de 249 tekstonderdelen met gedrag als hoofdcategorie, hebben er 223 een MoA-markering.

Vervolgens is bekeken hoe vaak iedere MoA voorkomt in het totaal. Van de 25 MoA's worden er 15 één of meermaals toegekend, zie figuur 4 hieronder voor de aantallen per MoA.

© Hogeschool Utrecht, 2026



Figuur 4: Aantallen tekstfragmenten per MoA in oplopende volgorde

Hoewel dit onderzoek geen kwantitatief onderzoek is, hebben we voor een indicatie van wat de meest relevante MoA's zijn tóch naar de aantallen gekeken. Wanneer bovenstaande figuur wordt bekeken dan springt één MoA er met kop en schouders bovenuit; *Social/ professional role & identity*.

© Hogeschool Utrecht, 2026

Vrij vertaald naar het Nederlands; Sociale en professionele rol en identiteit. Met als bijbehorende definitie (vrij vertaald vanuit het Engels): *Een samenhangend geheel van gedragingen en zichtbare persoonlijke eigenschappen van een persoon in een sociale- of werkomgeving.*
Deze definitie laat de continuïteit zien van persoonlijke eigenschappen en gedragingen in verschillende contexten. Met andere woorden, een reservist is zich ongeacht de context, blijvend bewust van zijn voorbeeldfunctie en het bijbehorende voorbeeldgedrag. Dit is een mooi aanknopingspunt voor een BCT waar tijdens gedragsinterventies op aangesloten kan worden: namelijk op het belang van de rol en identiteit van een reservist en het bijbehorende gedrag ongeacht de context of setting. Juist voor reservisten die functioneren in tenminste drie contexten; privé, werk en Defensie is dit van groot belang. Hiermee lijkt een aanknopingspunt voor de continuïteit van gedrag in verschillende contexten te zijn gevonden.

Een drietal andere MoA's 'scoort' redelijk gelijkwaardig. Allen zijn tussen de 25 en 35 keer gemarkeerd. Dit zijn;

- Waargenomen vatbaarheid/ kwetsbaarheid (*Perceived susceptibility/vulnerability*)
    - De perceptie van de waarschijnlijkheid dat men kwetsbaar is voor een dreiging.
- Overtuigingen over de gevolgen (*Beliefs about consequences*)
    - Overtuigingen over de gevolgen van een bepaald gedrag (d.w.z. opvattingen over wat er door het vertonen van een bepaald gedrag zal worden bereikt en/of verloren gaan, evenals de waarschijnlijkheid dat een bepaald gedrag tot een specifieke uitkomst zal leiden).
- Kennis (*Knowledge*)
    - Het besef dat iets bestaat

Ook dit drietal geeft belangrijke aanknopingspunten voor het inzetten van gedragsverandering bij reservisten. Te beginnen met kennis, het lijkt een open deur maar toch is het belangrijk om het via deze route bevestigd te krijgen. Het is immers lastig, zo niet onmogelijk om gedrag te veranderen of aan te passen wanneer je niet weet wat het gewenste gedrag is en wanneer dit ingezet dient te worden. Met andere woorden het is essentieel dat een reservist weet wat het gewenste digitaal veilige gedrag is en wanneer en hoe dit in te zetten. Al het voorgaande staat of valt met kennis.
Daarnaast lijkt de waarschijnlijkheid dat men kwetsbaar is voor een dreiging van belang. Dit gaat niet alleen over de eigen kwetsbaarheid maar ook over de kwetsbaarheid van de naasten. Vooral dat laatste aspect lijkt van belang. In de tekstfragmenten gaat het meermaals over "*Veiligheid -van- jezelf of gezin*". Soms wordt dit aangevuld met collega's binnen Defensie of Defensie zelf. Die focus op de veiligheid van anderen naast de eigen veiligheid is een toevoeging aan de theorie.
Ook overtuigingen over gevolgen van bepaald gedrag wordt relatief vaak in de tekstfragmenten gezien. Dat kan zowel gaan over gedrag dat leidt tot iets verliezen of juist bereiken. Deze MoA werkt twee kanten op. Het vertonen van onveilig gedrag kan leiden tot het verlies van iets, bijvoorbeeld de veiligheid van jezelf en/of van een ander. Het vertonen van veilig digitaal gedrag kan juist bijdragen tot verminderde kwetsbaarheid, van jezelf en/of je naasten en/of je werkgever(s) (inclusief Defensie).

De vier al besproken MoA's geven op basis van het huidige onderzoek de belangrijkste aanknopingspunten voor gedragsverandering. Desalniettemin is er een groep van vier andere MoA's die minder overtuigend naar voren komen uit de huidige analyse, maar wellicht interessant zijn voor veder onderzoek. Dit zijn.

- (Sociale) normen ((*Social) norms*)

© Hogeschool Utrecht, 2026

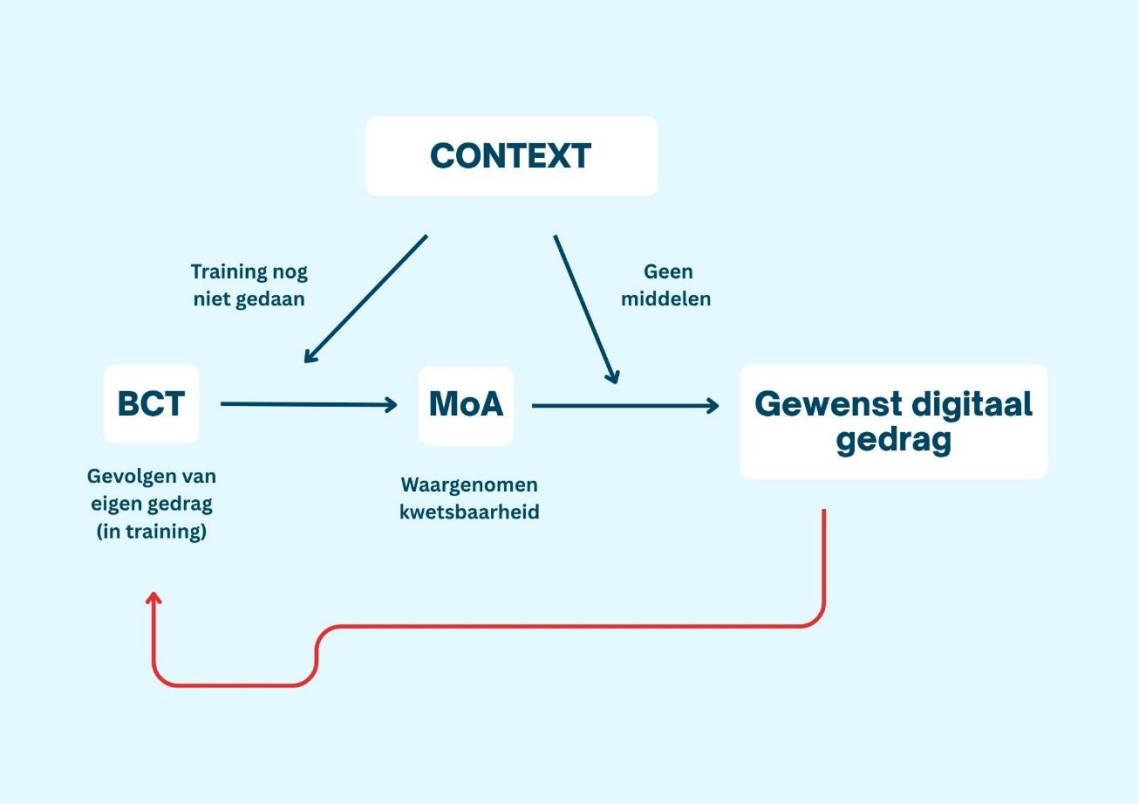
    - De houding en het gedrag van andere mensen binnen een sociale groep. De eigen perceptie van wat de meeste andere mensen binnen een sociale groep geloven en doen.
- Waarden (*Values)*
    - Morele, sociale of esthetische principes die door een individu of een samenleving worden aanvaard als leidraad voor wat goed, wenselijk of belangrijk is.
- Motivatie (*Motivation*)
    - Processen die verband houden met de drijfveer die gedrag een doel of richting geeft en die op bewust of onbewust niveau plaatsvinden.
- Omgevingscontext en hulpbronnen (*Environmental context & resources)*
    - Aspecten van iemands situatie of omgeving die het gedrag ontmoedigen of juist stimuleren.

Sociale normen lijken van belang. Het gaat daarbij om de houding en gedrag van anderen binnen de sociale groep. Binnen een organisatie als Defensie gaat het vaak over het belang van de groep (groot en klein) en de samenwerking tussen de personen in de groep. In de vacatures wordt het belang van het zijn van een teamspeler dan ook benadrukt. Wanneer het met name gaat over de groep en de groepsnorm dan verdiend dat aandacht. Bijvoorbeeld om dit positief in te zetten, de groepsnorm moet dan zijn dat men digitaal veilig gedrag vertoond. Of juist waken voor het verkeerde voorbeeld, dat de norm vervalt tot digitaal onveilig gedrag, zoals het meenemen van een (privé)telefoon op oefening/ missie tegen de instructies in.
Ook waarden zouden nader bestudeerd moeten worden. Waarden zijn principes die door een individu of een samenleving als goed/ wenselijk of belangrijk wordt ervaren. Door de opzet van het moreel beraad is bij iedere casus aandacht besteed aan de belangrijkste waarden met betrekking tot de casus. Juist deze door reservisten genoemde waarden, zowel persoonlijk als in relatie tot Defensie geven een belangrijk aanknopingspunt.
Motivatie zou ook interessant zijn om verder te verkennen. Wat is een interne of externe drijfveer voor reservisten om digitaal veilig gedrag te vertonen?
Ook de context is belangrijk Welke elementen uit de omgeving ontmoedigen of stimuleren (on)veilig gedrag? Dit speelt met name ook als reservisten de mogelijkheden niet hebben om het gewenste digitale gedrag te laten zien, bijvoorbeeld het openen van een dienstorder mag alleen op een Defensie device terwijl de reservist (nog) geen Defensie mobiele telefoon heeft.

MoA’s en bijbehorende Behavioural Change Techniques (BCT’s):

In bijlage 2 is al beschreven dat voor de meest gemarkeerde MoA’s de bijbehorende Behavioural Change Techniques (BCT’s) zijn bekeken in de *Theory and Techniques tool (TaTt).* Hierbij is alleen gekeken naar MoA’s en BCT’s met een in wetenschappelijk onderzoek bewezen significant verband. Twee onderzoekers hebben per MoA gekeken met welke BCT een bewezen link is en vervolgens bediscussieert en beargumenteert of deze BCT past bij de Defensieorganisatie en de doelgroep reservisten. Waarbij een generieke BCT de voorrang genoot ten opzichte van een specifiekere BCT, behalve als de specifiekere BCT beter aansloot op het profiel van de organisatie dan wel reservist. In figuur 5 nogmaals het eerder beschreven model, maar nu met voorbeeld van BCT en bijbehorende MoA. In tabel 4 hieronder is te zien welke MoA’s en BCT’s zijn gelinkt en of ze relevant worden geacht voor reservisten en Defensie.

© Hogeschool Utrecht, 2026



Figuur 5: Model met voorbeeld

Tabel 4: Mechanisms of Action met Behavioural Change Techniques

BCT's → MoA's ↓	Feed-back on out-come(s) of beha-viour	Social Support (un-speci-fied	Social sup-port (prac-tical	In-struc-tion on how to per-form beha-viour	Infor-mation about ante-ced-ents	Infor-mation about health conse-quences	Salience of con-se-quences Use methods speci-fically	Information about so-cial and en-vironmental conse-quences	Antici-pated regret	Infor-mation about emo-tional conse-quences	Pros and cons	Compar-ative im-agining of future out-comes	Non-spe-cific re-ward	Verbal per-sua-sion about ca-pabi-lity	Focus on past suc-ces
Knowledge	Ja	Misschien	Ja	Ja	Toe-komst of indi-rect		Ja		Mis-schien	Misschien					
Social/Profes-sional role & identity														Mis-schien	Ja
Beliefs about consequen-ces						Misschien	Ja	Misschien	Mis-schien	Misschien	Ja	Misschien	Ja		
Perceived susceptibi-lity/vulnerabi-lity							Ja								

Bij de MoA's *Sociale en professionele rol en identiteit* en *waargenomen kwetsbaarheid* zijn er slechts een of twee Behavioral Change Techniques met een bewezen verband. De BCT "Focus on past succes" linkt met de Sociale en professionele rol en identiteit. Salience of consequences heeft een bewezen link met waargenomen kwetsbaarheid.
De andere twee MoA's *kennis* en *overtuigingen over de gevolgen* hebben met meerdere BCT's een bewezen verband. Van de BCT's met een link lijken er meerdere aan te sluiten op het profiel van een reservist. Daarmee zijn ze waarschijnlijk te gebruiken zijn om gedragsverandering

© Hogeschool Utrecht, 2026

bij reservisten te stimuleren. De BCT die het meest in het oog springt is **salience of consequences**, deze heeft een bewezen verband met drie van de vier MoA's. De **consequenties of gevolgen** van je eigen gedrag, voor jezelf of voor een ander wegen zwaar voor reservisten. Van de overige BCT's lijken een aantal relevant. Zoals **instructie** hoe je dient te handelen, **feedback** op de uitkomst van het handelen en **sociale support**. Ook het maken van een overzicht van de **voor- en nadelen**, aandacht voor eerder behaalde **successen** en wellicht een **beloning** zijn allemaal passend. Deze gedragsveranderingstechnieken zijn wetenschappelijk onderbouwd en passen bij de doelgroep.

3.3 Juridisch onderzoek

Het juridische onderzoek is uitgevoerd door Kim My Tran als afstudeerproject voor haar Bachelor Recht. Bijlage 4 van dit rapport is een weergave van haar afstudeerproduct en daarin staat ook een verantwoording.

© Hogeschool Utrecht, 2026

Bijlage 4. Juridisch Onderzoek

Het juridische Onderzoek uitgevoerd door Kim My Tran is hieronder integraal over genomen

1.1 Inleiding

In een tijd waarin digitalisering toeneemt, nemen digitale dreigingen toe. Dit gebeurt ook in Nederland. Zo worden er cyberaanvallen uitgevoerd op Nederlandse doelen.[8] Hierbij spelen verschillende factoren een rol om de veiligheid te kunnen waarborgen. Eén van de factoren waarnaar gekeken wordt, is de menselijke factor. Zij vormen een belangrijke schakel in de veiligheidsketen van een organisatie, in dit geval het Ministerie van Defensie (hierna 'Defensie' genoemd). Bij Defensie wordt geïnvesteerd in de beveiliging van eigen systemen en in de training van het personeel. Echter, dit sluit niet uit dat er nog een kwetsbaar punt is, namelijk het digitale gedrag van medewerkers in hun privéleven.[9] In dit onderzoek ligt de focus op reservisten. Zij vormen een interessante groep, omdat zij naast hun werkzaamheden voor Defensie meestal nog een civiele baan en een privéleven hebben. Hiermee vormt de groep reservisten een voorbeeld van een grotere groep mensen die naast hun baan nog bijdragen aan het veiligheidsveld in Nederland. Anderen zijn bijvoorbeeld politievrijwilligers of brandweervrijwilligers.

Reservisten bij Defensie opereren voortdurend op het grensvlak tussen de civiele en de militaire wereld. Zij hebben een dubbelrol, wat hun risicoprofiel complexer maakt. Een realistisch scenario is het hergebruiken van één wachtwoord voor zowel je privéaccount, werkaccount als je Defensieaccount. Een reservist werkt bij bedrijf X als salesmanager. Op zijn werk heeft hij een inlognaam en wachtwoord voor zijn werkaccount. Tevens gebruikt hij hetzelfde wachtwoord in zijn privéleven, voor online accounts zoals Bol.com, Netflix en social media. Zelfs voor zijn Defensieaccount gebruikt hij hetzelfde wachtwoord. Bij een datalek van één van deze commerciële partijen kunnen deze inloggegevens op straat komen te liggen. Indien de identiteit van de persoon als reservist bekend is, kunnen kwaadwillenden deze gegevens misbruiken om toegang te verkrijgen tot informatie of digitale diensten van Defensie en haar medewerkers.[10] Hierdoor komt de veiligheid van Defensie in het geding. Het gevolg hiervan is dat mogelijk aanvallen worden gedaan op systemen van Defensie. Dit kunnen communicatiesystemen, navigatiesystemen, sensorsystemen en wapensystemen zijn, wat grote impact heeft op de staatsveiligheid.[11]

1.1.1 Opdrachtgever

De opdrachtgever voor dit onderzoek is het lectoraat Zorg en Veilig (hierna het Lectoraat genoemd) van de Hogeschool Utrecht. Het Lectoraat doet onderzoek naar het effectief aanpakken van ernstig overlastgevend gedrag. Hiervoor werkt het samen met partners uit het onderwijs, het onderzoek en de praktijk, zoals de Politie Midden-Nederland, Bureau Regionale Veiligheidsstrategie en het Platform Sociaal Domein van de VNG.[12] Het Lectoraat heeft als aandachtspunt ook privacy en gegevensgebruik in het publieke domein.

Vanaf 1 oktober 2025 heeft het Lectoraat een project lopen tot en met 30 september 2026: *"Gedragsverandering voor digitale veiligheid".* Dit project wordt in samenwerking met het lectoraat Cyber Security (HU), Awareways en het Defensie Cyber Warfare and Training Centre (CWTC) uitgevoerd.[13] Het lectoraat Cyber Security (HU) richt zich op de organisatorische inrichting en interventies op het gebied van technologie en het veiliger kunnen maken van digitaal menselijk

[8] 'Cybersecuritybeeld Nederland 2025', nctv.nl.
[9] Van den Berg, p. 7.
[10] Van den Berg, p. 17.
[11] 'Bedreigingen in de digitale omgeving', Defensie.nl.
[12] 'Lectoraat zorg en veiligheid', hu.nl.
[13] 'Gedragsverandering voor digitale veiligheid', hu.nl.

© Hogeschool Utrecht, 2026

gedrag.[14] Awareways is een organisatie die zich richt op digitale weerbaarheid.[15] Tot slot is het Defensie Cyber Warfare and Training Centre (CWTC) een centrale expertisecentrum en opleidingsinstituut van het Defensie Cyber Commando (DCC).[16]

Het doel van dit onderzoek is om veelbelovende gedragsveranderingstechnieken te identificeren die het digitaal gedrag van reservisten in hun privéleven, bij hun civiele baan en bij Defensie veiliger maken. Hiervoor wordt er gekeken naar de juridische toelaatbare grenzen. De doelgroep van dit onderzoek zijn de reservisten bij Defensie. Zij vormen een unieke en groeiende groep binnen Defensie, omdat zij nog een civiele baan en een privéleven naast Defensie hebben.

Praktijkprobleem
Binnen Defensie wordt er onderscheid gemaakt tussen burgermedewerkers, beroepsmilitairen en reservisten. Burgermedewerkers hebben in tegenstelling tot de beroepsmilitairen en reservisten een niet-militaire functie.[17] Een groot deel van het rechtspositionele kader van de burgermedewerker is vastgelegd in de Wet ambtenaren Defensie en het Burgerlijk ambtenarenreglement Defensie. Daarnaast zijn er ook delen van de Ambtenarenwet 2017 die van toepassing zijn op de burgermedewerkers.[18] Reservisten daarentegen vallen juridisch gezien onder dezelfde wetgeving als militair personeel.[19]

Defensie ziet een structurele groei in het aantal reservisten. Zij hebben naast hun taken bij Defensie ook nog een civiele baan in tegenstelling tot de beroepsmilitair. Hierdoor is hun dagelijks leven ook anders ingericht dan bij een beroepsmilitair. Afhankelijk van het type reservist werkt die enkele weken per jaar voor Defensie of soms 20 uur per week of meer. Deze hybride positie zorgt ervoor dat een reservist voortdurend schakelt tussen de civiele en de militaire wereld. Wanneer zij niet bij Defensie zijn, stemmen zij hun gedrag logischerwijze af op de normen van hun civiele werkgever of hun privésituatie. Deze hybride positie creëert een grijs gebied waarin het digitale gedrag van een reservist in de privésfeer of bij de civiele baan onbedoeld een risicofactor wordt voor de veiligheid van Defensie. Het digitale gedrag van een reservist buiten diensttijd, zoals het gebruik van social media, heeft direct invloed op de cyberveiligheid van Defensie, met name de veiligheid van systemen en informatie.[20] Met digitaal gedrag wordt verwezen naar handelingen en activiteiten die een persoon uitvoert in de digitale wereld, zoals het bezoeken websites, het kijken van filmpjes en het inloggen op social media.[21]

Een ander scenario naast het hergebruiken van wachtwoorden is het synchroon houden van een Defensie agenda met een civiele baan agenda en een privéagenda. Het handmatig overnemen van afspraken is tijdrovend, waarbij een reservist steeds moet nadenken over hoe hij de Defensieafspraak dan in zijn werk- of privéagenda zet. Een reservist zou niet zomaar een automatische koppeling moeten gebruiken om zijn agenda's synchroon te houden, want hierdoor kan er gevoelige informatie van Defensie onbedoeld naar publieke cloudomgevingen worden gelekt. Het kernprobleem is dat Defensie het digitale gedrag van de reservist buiten diensturen niet zomaar kan reguleren. Dit gaat om hun digitale gedrag in hun privéleven en bij hun civiele baan. Binnen Defensie kunnen reservisten aangestuurd worden via strikte instructies en de sociale norm van Defensie, zoals de Gedragscode Defensie en het Handboek Cyberveilig gedrag Defensie. Echter, deze gedragsmechanismes komen te vervallen zodra een reservist zich in de privésfeer of bij zijn civiele werkgever bevindt.

[14] 'Cyber Security', hu.nl.
[15] 'Onze aanpak', awareways.com.
[16] 'Defensie Cyber Commando', Defensie.nl.
[17] 'Burgermedewerker', werkenbijDefensie.nl.
[18] Aarts & Fink 2025.
[19] 'Wat is een reservist?', Defensie.nl.
[20] 'Gedragsverandering voor digitale veiligheid', hu.nl.
[21] Rountree 2013, par. 1.2.2.1.

© Hogeschool Utrecht, 2026

Momenteel ontbreekt een duidelijk juridisch kader dat de reikwijdte van de instructiebevoegdheid van Defensie in de privésfeer definieert. Bestaande richtlijnen en trainingen zijn buiten diensttijd nauwelijks afdwingbaar of controleerbaar. Hierdoor is er een behoefte aan een juridisch fundament en werkzame gedragsmechanismes die reservisten stimuleren om uit zichzelf hun digitale gedrag aan te passen om de veiligheid van Defensie te waarborgen.[22]

1.1.2Juridisch kader

Handboek Cyberveilig gedrag Defensie
Het handboek Cyberveilig gedrag Defensie is er om Defensiemedewerkers een overzicht te geven van richtlijnen op het gebied van cyberveiligheid. Het is van belang om Defensiemedewerkers voor te lichten op het gebied van cybersecurity en het veilig handelen. Het handboek hanteert cyberveilig gedrag als veilig gedrag dat wordt vertoond in het gebruik van ICT-middelen, al dan niet gekoppeld aan interne en/of externe netwerken.[23]

Gedragsregels Defensie Sociale Veiligheid & Integriteit
De Gedragsregels Defensie Sociale Veiligheid & Integriteit zijn gebaseerd op de kernwaarden van Defensie zoals verbondenheid, veiligheid, vertrouwen en verantwoordelijkheid. In dit document staan verschillende thema's van gedrag. Ook staan er regels in over hoe iedereen die bij Defensie werkt in zijn privéleven en vrije tijd moet gedragen en het zorgvuldig en integer omgaan met gebruik van Defensiemiddelen. Het overtreden van deze regels kan leiden tot tuchtrechtelijke maatregelen.[24]

Gedragscode Defensie
In de Gedragscode Defensie staat dat de waarden voor iedereen binnen Defensie gelden. Daarnaast staat er ook in hoe een medewerker zich moet gedragen op het internet. Een belangrijke waarde binnen de Gedragscode Defensie is veiligheid. Hieronder valt ook veilig werken en dit geldt ook voor digitaal gedrag.[25]

Artikel 7 Grondwet
In artikel 7 van de Grondwet wordt het recht van vrijheid van meningsuiting geregeld. Hierin staat dat iedereen het recht heeft om gedachten of gevoelens te openbaren. Dit recht kan worden beperkt, wanneer dit in de wet staat voorgeschreven.

Artikel 10 Grondwet
In artikel 10 van de Grondwet staat het recht op privacy. Dit beteken dat iedereen recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Hierbij gaat het niet alleen om fysieke privacy, maar ook de bescherming van persoonsgegevens. Dit recht kan worden beperkt, wanneer dit in de wet staat voorgeschreven.

Artikel 12a Wet ambtenaren Defensie (WAD)
Door de speciale positie van militairen en reservisten kunnen hun grondrechten worden beperkt op grond van artikel 12a van de Wet ambtenaren Defensie. Dit gaat om het openbaren van gedachten of gevoelens als het recht op vereniging, tot vergadering en tot betoging.

[22] Projectvoorstel KIEM Defensie, indieningsronde april t/m september 2025.
[23] Van den Berg, p.7.
[24] Ministerie van Defensie 2019.
[25] Ministerie van Defensie 2018.

© Hogeschool Utrecht, 2026

Artikel 12bis Wet ambtenaren Defensie (WAD)
Op grond van artikel 12bis van de Wet ambtenaren Defensie is het dat een militaire ambtenaar zich als goed militair ambtenaar dient te gedragen en het bevoegde gezag dient zich als een goede werkgever te gedragen.

Artikel 34 Algemeen militair ambtenarenreglement (AMAR)
Artikel 34 lid 1 sub b van het Algemeen militair ambtenarenreglement regelt dat een militair kan worden geschorst als hij een strafbaar feit heeft gepleegd op grond van de Wet militair tuchtrecht. Daarnaast kan een militair ook geschorst worden als er een strafrechtelijke vervolging van een misdrijf tegen hem is ingesteld op grond van artikel 34 lid 2 sub a van het Algemeen militair ambtenarenreglement.

Artikel 39 Algemeen militair ambtenarenreglement (AMAR)
In artikel 39 lid 2 sub k en sub l van het Algemeen militair ambtenarenreglement staat dat een militair kan worden ontslagen op grond van nalatigheid in de vervulling van zijn plichten. Een andere grond voor ontslag is wegens wangedrag in de dienst en buiten de dienst. Dit gedrag is schadelijk voor zijn dienstvervulling of is niet in overeenstemming met het aanzien van zijn ambt.

Artikel 18 Wet militaire tuchtrecht (WMT)
De Wet militaire tuchtrecht stelt dat militairen kunnen worden gestraft voor misdrijven en dienstverzuimen. In artikel 18 van de Wet militaire tuchtrecht staat dat het niet opvolgen van een dienstvoorschrift in strijdt is met de militaire tucht. Dit artikel is relevant als er blijkt dat de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag Defensie als dienstvoorschriften worden gezien

Artikel 135 Wetboek van Militair Strafrecht (WMSr)
Binnen Defensie zijn er dienstvoorschriften, dit is een schriftelijk besluit van algemene strekking waarin een gebod of verbod in staat gericht aan alle of een groep militairen grond van artikel 135 van het Wetboek van Militair Strafrecht.

Artikel 137 lid 1 Wetboek van Militair Strafrecht
In artikel 137 lid 1 van het Wetboek van Militair Strafrecht staat dat het een misdrijf is als een militair het dienstvoorschrift niet opvolgt. Waardoor er gevaar is voor personen of goederen, dan kan hij gestraft worden met een gevangenisstraf of hechtenis van ten hoogste drie maanden of een geldboete van de tweede categorie.

1.1.4 Doelstelling met beoogd beroepsproduct

De uitkomsten van het onderzoek worden gebruikt voor het beroepsproduct. In dit geval is het beoogd beroepsproduct uiteindelijk een infographic folder of poster. Voor de opdrachtgever is het van belang dat het beroepsproduct duidelijk en makkelijk te begrijpen is. Het beroepsproduct maakt duidelijk zichtbaar wat de juridische grenzen zijn van Defensie op het gebied van het reguleren van digitaal gedrag van reservisten in hun privéleven en bij hun civiele baan.

Het beroepsproduct is voor Defensie. Zij kunnen zien wat de juridische grenzen zijn en welke stappen ze kunnen ondernemen. Daarnaast is het ook mogelijk om dit beroepsproduct te gebruiken om reservisten te informeren op het gebied van digitaal gedrag. Ze worden geïnformeerd over wat Defensie juridisch gezien wel en niet mag op het gebied van het reguleren van hun digitaal gedrag in hun privéleven en bij hun civiele baan.

Aangezien het voor zowel Defensie als reservisten toepasbaar is, kan het beroepsproduct getest worden bij Defensie of reservisten. De infographic folder of poster is makkelijk om onderling

© Hogeschool Utrecht, 2026

te verspreiden. Folders kunnen zowel fysiek als digitaal worden verstuurd en posters kunnen opgehangen worden op plekken waar reservisten vaak aanwezig zijn. Het beroepsproduct kan getest worden doormiddel van een enquête of een verzameling van feedback. Het verzamelen van feedback kan tijdens een consortiumbijeenkomst waar onder andere de professionals van Awareways en de contactpersoon van Defensie aanwezig zijn. Met het opgeleverde resultaat kan het beroepsproduct aangepast worden waar nodig is. Gaandeweg kan het zijn dat het beroepsproduct wordt aangepast om beter aan te sluiten aan de wensen van de opdrachtgever.

Centrale vraag

In hoeverre mag Defensie het digitale gedrag van reservisten in hun privéleven en bij hun civiele baan beperken op grond van het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie, artikel 12a jo. 12bis van de Wet ambtenaren Defensie, artikel 18 van de Wet militair tuchtrecht en jurisprudentie gelet op de bescherming van de persoonlijke levenssfeer op grond van artikel 10 van de Nederlandse Grondwet, met het doel om de veiligheid van Defensie te waarborgen?

Deelvragen

De centrale vraag wordt beantwoord aan de hand van de volgende deelvragen:

Praktijkdeelvraag:

1. Welke maatregelen neemt Defensie nu om het digitaal gedrag van reservisten veilig te laten verlopen in hun privéleven en bij hun civiele baan ten behoeve van de veiligheid van Defensie?

Onderzoek van het recht deelvragen:

2. In hoeverre bepalen het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie en de Gedragscode Defensie welke plichten reservisten hebben met betrekking tot hun digitale gedrag binnen hun functie en in hun privéleven en bij hun civiele baan en is dit evenredig gelet op artikel 12a jo. 12bis van de Wet ambtenaren Defensie?
3. In hoeverre kunnen het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie en de Gedragscode Defensie als een dienstvoorschrift worden gezien in de zin van artikel 135 van het Wetboek van Militair Strafrecht jo. artikel 18 van de Wet militair tuchtrecht en gelden de gedragsnormen hierin voor reservisten zowel tijdens hun dienst binnen Defensie als in hun privéleven en bij hun civiele baan gelet op artikel 10 van de Nederlandse Grondwet?
4. In hoeverre mag Defensie het gedrag van reservisten in hun privéleven en bij hun civiele baan beperken op grond van jurisprudentie ten behoeve van de veiligheid van Defensie?

1.1.5 Leeswijzer voor het rapport

Voor het beantwoorden van de centrale vraag wordt in hoofdstuk 2 deelvraag 1 beantwoord door middel van een praktijkonderzoek. Dit is aan de hand van een documentenonderzoek van de interne richtlijnen, een observatieonderzoek van twee moreel beraden en een interview. Vervolgens wordt in hoofdstuk 3 deelvraag 2 beantwoord. Er wordt eerst gekeken naar de reikwijdte en proportionaliteit van de interne richtlijnen van Defensie voor reservisten in samenhang met de Wet ambtenaren Defensie. Dit is aan de hand van literatuur en het documentenonderzoek van hoofdstuk 2. In hoofdstuk 4 wordt deelvraag 3 beantwoord door literatuur, kamerstukken, wetgeving en jurisprudentie te onderzoeken. Hierbij is het van belang om eerst te kijken wat de wet aanmerkt als een dienstvoorschrift, om vervolgens te kijken of de huidige interne richtlijnen

© Hogeschool Utrecht, 2026

van Defensie als een dienstvoorschrift kunnen worden gezien. Vervolgens wordt in hoofdstuk 5 aan de hand van jurisprudentie onderzoek deelvraag 4 beantwoordt. Tot slot wordt in hoofdstuk 6 de eindconclusie behandelt als antwoord op de centrale vraag met aanbevelingen.

1.2 Huidige maatregelen bij Defensie

51.2.1 Inleiding

Dit hoofdstuk behandelt deelvraag 1, '*Welke maatregelen neemt Defensie nu om het digitaal gedrag van reservisten veilig te laten verlopen in hun privéleven en bij hun civiele baan ten behoeve van de veiligheid van Defensie?'* aan de hand van een praktijkonderzoek. Als eerste wordt er in paragraaf 2.2 onderzoek gedaan naar de huidige interne richtlijnen van Defensie op het gebied van (digitaal) gedrag. Het gaat hierbij om de Gedragscode Defensie, de Gedragsregels Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag Defensie. Vervolgens wordt in paragraaf 2.3 een observatieonderzoek van twee moreel beraden behandeld. In paragraaf 2.4 wordt het interview behandeld en tot slot staat de tussenconclusie in paragraaf 2.5.

1.2.2 Documentenonderzoek

In deze moderne tijd waarin technologie geavanceerder wordt, neemt de noodzaak voor cyberveiligheid toe. In Nederland zijn cyberdreigingen toegenomen en hierbij is Defensie dagelijks doelwit van cyberaanvallen.[26] Om de eigen digitale veiligheid van Defensie te waarborgen, heeft Defensie drie taken in het cyberdomein. De eerste taak is eigen cyberveiligheid in alle omstandigheden. Dit betekent dat Defensie de eigen systemen veilig moet houden als dagelijks doelwit van verschillende aanvallen. De tweede taak is het uitvoeren van militaire cyberoperaties. Dit houdt in dat het cyberdomein een operationeel domein is waarin militaire operaties worden uitgevoerd. De laatste taak is cyberweerbaarheid van het Koninkrijk en bondgenoten. Defensie moet zich continu verdedigen tegen hybride dreigingen, omdat het een specifieke rol speelt bij de cyberweerbaarheid van het Koninkrijk en bondgenoten.[27] Om de veiligheid van Defensie te waarborgen, zijn er binnen Defensie interne richtlijnen voor veilig digitaal gedrag. Met digitaal gedrag wordt verwezen naar handelingen en activiteiten die een persoon uitvoert in de digitale wereld. Voorbeelden hiervan zijn het bezoeken van websites, het kijken van filmpjes en het inloggen op social media.[28] Om het digitaal gedrag van Defensiemedewerkers, waaronder ook reservisten veilig te laten verlopen, zijn er interne richtlijnen, namelijk de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag Defensie.

Gedragscode Defensie[29]

Defensie vecht voor vrede en veiligheid. Hierbij is het van belang dat het duidelijk is waar ze voor staan. In de Gedragscode Defensie staan de basiswaarden over hoe al het personeel met elkaar, anderen, middelen en bevoegdheden omgaan. Deze basiswaarden gelden voor iedereen, op de werkvloer, op uitzending, op de kazerne en in de top van de organisatie. Hierbij is er geen onderscheid tussen personeel met of zonder militaire functie. De vier basiswaarden die in de Gedragscode Defensie staan zijn verbondenheid, veiligheid, vertrouwen en verantwoordelijkheid.[30]

1. Verbondenheid

[26] Ministerie van Defensie 2025, p.3.
[27] Ministerie van Defensie 2025, p.3.
[28] Rountree 2013, par. 1.2.2.1.
[29] Bijlage 1: Gedragscode Defensie.
[30] Ministerie van Defensie 2018.

© Hogeschool Utrecht, 2026

De eerste waarde staat voor samenwerken, anderen helpen, openstaan voor feedback en elkaar aanspreken. Bij Defensie draait het om verbondenheid en kameraadschap, door elkaar te coachen en aan te spreken op het werk en het gedrag.

2. Veiligheid

Veiligheid staat voor veilig werken. Dit betekent geldende procedures verstandig toepassen en respectvol met een ander omgaan. Daarnaast moet onveilig of ongewenst gedrag bespreekbaar worden gemaakt of dit worden gemeld voor een veilige organisatie.

3. Vertrouwen

De derde waarde is vertrouwen. Dit houdt in dat het personeel nauwkeurig werkt, zorgvuldig omgaat met middelen en bevoegdheden en eerlijk en open met elkaar communiceert. Hierbij wordt van het personeel verwacht dat zij zich bewust zijn van hun voorbeeldfunctie en de hoge eisen die de samenleving stelt aan hun gedrag, of het nu in dienst is of erbuiten, op uitzending, of op internet.

4. Verantwoordelijkheid

Tot slot is er nog de waarde verantwoordelijkheid. De medewerkers van Defensie dragen een grote verantwoordelijkheid. Dit houdt in dat taken worden uitgevoerd en kwaliteit wordt geleverd. Het personeel is verantwoordelijk voor het eigen gedrag en er wordt aangespoord om het beste uit zichzelf en elkaar te halen.

1.2.4Gedragsregels Defensie Sociale Veiligheid & Integriteit

De Gedragsregels Defensie Sociale Veiligheid & Integriteit is een interne richtlijn van Defensie over het zorgvuldig omgaan met bevoegdheden, taken, met elkaar, met anderen en met middelen. De gedragsregels die in de Gedragsregels Defensie Sociale Veiligheid & Integriteit staan zijn ter verduidelijking van de waarden die in de Gedragscode Defensie staan. Het in strijd handelen met de Gedragscode Defensie of het overtreden van de regels kunnen leiden tot gevolgen. Afhankelijk van de overtreding kan er aangifte worden gedaan of er wordt mogelijk opgetreden volgens de Wet Militair Tuchtrecht of de (militaire) Ambtenarenwet. In deze interne richtlijn staan acht verschillende thema's met regels, praktijkvoorbeelden, hulpvragen en wet- en regelgeving. Voor dit adviesrapport zijn vijf thema's relevant, waardoor alleen deze vijf behandeld worden.[31]

1. Gedrag in vrije tijd

Iedereen heeft het recht op een privéleven. Echter, als Defensiemedewerker kunnen bepaalde gedragingen en situaties in de vrije tijd risicovol zijn voor jezelf en voor Defensie. Ten eerste moet een Defensiemedewerker zich bewust zijn van de risico's van social media. Dit betekent dat hij rekening houdt met hoe hij als Defensiemedewerker overkomt op social media. Dit kan in verband worden gebracht met zijn krijgsmachtdeel, eenheid, functie of afdeling. Ten tweede vermijd je als Defensiemedewerker bepaalde gelegenheden of personen in de privéomgeving. Dit zijn personen die regelmatig de wet overtreden of die verbonden zijn aan een verboden vereniging. Als laatste moet een Defensiemedewerker niet in een chantabele of anderszins kwetsbare positie terechtkomen. Financiële problemen kunnen een Defensiemedewerker chantabel maken. Dit thema hangt samen met de waarde, vertrouwen, uit de Gedragscode Defensie.

Een praktijkvoorbeeld is dat een Defensiemedewerker een enthousiast motorrijder is. Zijn buurman vraagt of hij mee wil doen aan een motortour om geld op te halen voor een doel. Hij stemt hier mee in, maar tijdens een voorbereidende bijeenkomst blijken er veel leden van enkele

[31] Ministerie van Defensie 2019, p.2-3.

© Hogeschool Utrecht, 2026

omstreden motorclubs aanwezig te zijn. Is het verstandig als de Defensiemedewerker dan nog meerijdt?[32]

2. Zorgvuldig gebruik van Defensiemiddelen

Voor werk is het mogelijk om gebruik te maken van allerlei middelen van Defensie. Medewerkers moeten hier voorzichtig, zuinig en doelgericht mee omgaan. Hierbij zijn er verschillen in het gebruik van middelen. Zo is het gebruik van een dienstauto uitsluitend voor werkdoeleinden. Daarentegen mag een diensttelefoon na redelijkheid ook privé worden gebruikt, indien dit het dienstbelang niet schaadt. Deze regels vallen onder de waarde, verantwoordelijkheid uit de Gedragscode Defensie.

Een praktijkvoorbeeld is dat een Defensiemedewerker voor het 40-jarige huwelijksfeest van zijn ouders een filmpje wil laten zien van de kleinkinderen. Op het werk staat een nauwelijks gebruikte beamer. Leent de Defensiemedewerker deze voor het feest?[33]

3. Nevenwerkzaamheden

Als Defensiemedewerker is het mogelijk om maatschappelijk betrokken te zijn. Een Defensiemedewerker kan in privétijd als Zzp'er werken of actief betrokken zijn bij een vereniging, stichting of bedrijf. Deze nevenwerkzaamheden kunnen bepaalde risico's met zich meebrengen. Onder nevenwerkzaamheden vallen zowel betaalde als onbetaalde activiteiten, zoals vrijwilligerswerk of een hobby. De eerste belangrijke regel is dat de nevenwerkzaamheden besproken worden met de leidinggevende, zodat er afspraken worden gemaakt over het nevenwerk of het wordt niet toegestaan. Daarnaast voert een Defensiemedewerker geen nevenwerk uit dat niet samengaat met een (militaire) functie. Dit thema valt onder de waarde, verantwoordelijkheid uit de Gedragscode Defensie.

Een praktijkvoorbeeld is dat een collega naast zijn werk bij Defensie gestart is met een kleine sportschool in de buurt van de basis. Hij is gespecialiseerd in vechtsporten en ter promotie nodigt hij op de kazerne mensen uit om een aantal gratis lessen te krijgen. Neem je als Defensiemedewerker dit aanbod aan?[34]

4. Contacten met bedrijfsleven

Defensiemedewerkers kunnen contact hebben met bedrijven. Sommige Defensiemedewerkers kunnen opdrachten geven aan het bedrijfsleven en hebben daarom contact met het bedrijfsleven. Het is belangrijk om (de schijn van) belangenverstrengeling en oneerlijke concurrentie te voorkomen. Dit valt onder de waarde, verantwoordelijkheid uit de Gedragscode Defensie.

Een praktijkvoorbeeld is dat een oud-collega voor een bedrijf werkt dat producten levert aan Defensie. Er loopt een aanbesteding en hij belt je op met de vraag om extra informatie, zodat hij zijn offerte op maat kan maken. Wat doe je?[35]

5. Zorgvuldig omgaan met informatie

Het is van belang dat Defensiemedewerkers zorgvuldig omgaan met informatie, omdat ze toegang hebben tot allerlei vertrouwelijke informatie. Samenwerkingspartners, collega's en de samenleving moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met informatie, in het belang van de (nationale) veiligheid. Zo geldt dat informatie alleen wordt gebruikt voor de uitoefening van de functie en dat de Defensiemedewerker zich houdt aan de kaders van wet- en

[32] Ministerie van Defensie 2019, p.10-12.
[33] Ministerie van Defensie 2019, p.13-15.
[34] Ministerie van Defensie 2019, p.19-21.
[35] Ministerie van Defensie 2019, p. 22-24.

© Hogeschool Utrecht, 2026

regelgeving. Daarnaast wordt vertrouwelijke informatie goed opgeborgen en wordt gezorgd dat niemand zomaar meekijkt of meeluistert tijdens de werkzaamheden. Ook heeft een Defensiemedewerker geen direct contact met de media of politici. Deze regels vallen onder de waarde verantwoordelijkheid van de Gedragscode Defensie.

Een praktijkvoorbeeld is dat een Defensiemedewerker tijdens een uitzending een paar mooie foto's heeft gemaakt van de omgeving van de basis. Een collega heeft gevraagd of hij deze foto's mag hebben voor zijn thuisfront. De dag erna kom je erachter dat hij deze op facebook heeft gedeeld. Wat vind je hiervan?

In de Gedragsregels Defensie Sociale Veiligheid & Integriteit staat specifiek dat werken bij Defensie ook verwachtingen en verantwoordelijkheden met zich meebrengen en dat personeel zich op een bepaalde manier dient te gedragen, zowel in werk- als privétijd. Bij het afleggen van de eed of belofte is er gehoorzaamheid aan de wetten en onderwerping aan de krijgstucht gezworen of beloofd. Er wordt ook concreet vermeld dat het in strijd handelen met de Gedragscode Defensie of het overtreden van de regels consequenties opleveren. Afhankelijk van de overtreding kan er aangifte gedaan worden of wordt mogelijk opgetreden conform de Wet Militair Tuchtrecht of de (militaire) Ambtenarenwet.[36]

1.2.5Handboek Cyberveilig gedrag Defensie

Het Handboek Cyberveilig gedrag Defensie is een richtlijn om Defensiemedewerkers voor te lichten over het belang van cybersecurity. Hierdoor wordt beveiliging op dit gebied een logisch verhaal en wordt veilig handelen daarmee bevorderd. Cybergedrag valt onder gezamenlijke normen en waarden bij Defensie en behoort het vandaag de dag tot een randvoorwaarde voor militaire operaties. Er wordt verwacht dat Defensiemedewerkers de kennis uit het handboek tot zich nemen. Het handboek geeft een overzicht van richtlijnen op het gebied van cyberveiligheid en concrete handvatten om het werk zo veilig mogelijk te doen en te houden.[37]

Het Handboek Cyberveilig gedrag Defensie bestaat uit een aantal thema's hoe Defensiemedewerkers cyberveilig kunnen handelen, op het werk en thuis. Elk thema weerspiegelt de werkelijke situaties waar Defensiemedewerkers mee in aanraking komen of kunnen komen. Daarnaast worden in elk thema de persoonlijke en organisatierisico's van onveilig gedrag behandeld en worden er veilige principes en tips tegenover gezet. Echter, als het gaat om cyberveilig gedrag is het onderscheid tussen werk- en privésituatie niet altijd scherp te krijgen. Niet alle risico's en tips gelden voor elke situatie, de principes wel.[38]

Het Handboek Cyberveilig gedrag Defensie is niet openbaar, de thema's worden in overleg met Defensie slechts op een algemene manier beschreven. Het openbaar maken van de specifieke tips zou kunnen leiden tot extra risico's voor Defensie en dat mag dus niet.

1.2.6 Observatieonderzoek

Als onderdeel van het praktijkonderzoek voor dit adviesrapport zijn op vrijdag 13 februari 2026 en vrijdag 29 mei 2026 een moreel beraad gehouden. Het moreel beraad houdt in dat er een dilemma wordt voorgelegd in de vorm van een casus. Aan de hand van de casus gaan de reservisten nadenken over het dilemma en geven zij aan wat zij ervan vinden of wat zij zouden doen. Bij het eerste moreel beraad waren er 11 reservisten aanwezig en bij het tweede moreel beraad 9 reservisten. Het doel van deze observatie is om diepgaand inzicht te krijgen in wat reservisten

[36] Ministerie van Defensie 2019, p.3.
[37] Van den Berg, p.5.
[38] Van den Berg, p.7.

© Hogeschool Utrecht, 2026

zelf moreel goed en acceptabel vinden als het gaat om het reguleren van het digitale gedrag van reservisten in de privésfeer.

Moreel beraad 1
Tijdens het moreel beraad zijn de reservisten verdeeld in twee groepen met ieder een eigen casus. Mijn observatie ging over een groep bestaande uit vijf actief participerende reservisten bij casus 1 over het hergebruiken van wachtwoorden.[39]

Uit de verzamelde observatiedata kwamen enkele belangrijke punten naar voren die van belang zijn voor het adviesrapport. Zo is er onder de reservisten een hoog bewustzijn van digitale dreigingen, zoals het risico op tracking of de kans op chantage. Toch bleek dat reservisten in de privésfeer soms kiezen voor comfort en gemak boven strikte veiligheid, bijvoorbeeld het hergebruiken van simpele wachtwoorden of het delen van wifi-netwerken met derden, vaak vrienden en familie. Uit de observatie bleek een verschil te zijn tussen theorie en praktijk. Een voorbeeld is het meenemen van een privélaptop tijdens uitzending zodat tijdens de uitzending nog wat geregeld kon worden voor het eigen bedrijf, terwijl het bij sommige krijgsmachtonderdelen verboden is om privéapparaten mee te nemen.

Als het gaat om mogelijke oplossingen, is het duidelijk dat de reservisten voor deze casus, het te ver vinden gaan als hun privacy wordt geschonden met hele harde controles en het opvragen van privéwachtwoorden. Dit lijkt hen ook niet veilig, aangezien deze gegevens dan bewaard worden. Toch lijken andere reservisten wel open te staan voor een vorm van controle. De groep reservisten bij dit moreel beraad heeft over het algemeen een voorkeur voor een stimulerende rol vanuit Defensie en dit wordt dit gezien als een vorm van goede zorg vanuit de werkgever.

Moreel beraad 2
Bij het tweede moreel beraad waren er 9 reservisten aanwezig. De casus ging over het synchroon houden van 3 agenda's, namelijk de privéagenda, werkagenda en Defensieagenda.[40]
Uit het moreel beraad is naar voren gekomen dat het niet mogelijk is om de Defensieagenda te synchroniseren met de privéagenda. Echter, het is wel mogelijk om de Defensieagenda te exporteren en in de privéagenda of werkagenda te importeren. Dit is niet relevant voor alle reservisten, aangezien de inhoud van de Defensieagenda sterk verschilt per reservist. De afspraken en afspraakbeschrijvingen zijn afhankelijk van de functie van de reservist. Een reservist met een hogere functie heeft meer vertrouwde informatie staan in de Defensieagenda. Naast de afspraken hebben reservisten ook een jaarrooster, waar de algemene afspraken staan.

Bij deze groep reservisten geven ze aan dat ze zelf hun Defensieafspraken handmatig overnemen in hun privéagenda of werkagenda door alleen de begin- en de eindtijd te noteren. Dit is ten behoeve voor hun eigen privé- of werkplanning. Hierbij vinden ze het niet verantwoord om de locatie, inhoud of codes van de afspraak te noteren. Volgens deze reservisten is alleen een tijdsblok al voldoende. Wanneer de reservist voor een langere tijd weggaat en hierdoor onbereikbaar is, geeft de reservist wel de locatie door aan het thuisfront. Er wordt ook doorgegeven wie de contactpersoon is. Voor de rest geven reservisten aan dat ze bijna geen informatie delen met hun partner om henzelf en het thuisfront veilig te houden.

Interview
Naast het documentenonderzoek en het observatieonderzoek is er een interview gehouden om een visie te krijgen over het huidige beleid van Defensie met betrekking tot het digitaal gedrag van reservisten. Hierbij is er een interview gehouden met een Defensiemedewerker van de

[39] Bijlage 2: Observatieverslag moreel beraad 1.
[40] Bijlage 3: Observatieverslag moreel beraad 2.

© Hogeschool Utrecht, 2026

afdeling Beleid en Analyse bij het Kenniscentrum van de Centrale Organisatie Integriteit Defensie (COID).[41][42] Uit het interview is naar voren gekomen dat reservisten juridisch gezien onder dezelfde integriteitskaders vallen als het beroepspersoneel, omdat zij ook een militaire functie hebben. Er is wel een verschil in de risico's bij een beroepsmilitair en een reservist doordat een reservist vaak opereert tussen Defensie en de civiele sector. Dit is belangrijk binnen de context van de 'Adaptieve Krijgsmacht', namelijk de flexibele schil van reservisten die Defensie de komende jaren substantieel wil uitbreiden. Doordat het budget van Defensie sterk gegroeid is, zijn zij een zeer interessante marktpartij geworden, wat het risico op belangenverstrengeling en misbruik van gevoelige informatie bij reservisten met commerciële nevenfuncties kan vergroten.

Daarnaast is uit het interview naar voren gekomen dat binnen Defensieterreinen er controle kan worden gehouden op Defensienetwerken en dat activiteiten op dit netwerk worden gelogd. Defensie heeft geen grip op het digitale gedrag van reservisten in de privésfeer. Voordat een reservist aangenomen wordt, wordt er een veiligheidsscreening gedaan door de MIVD of AIVD. Echter, achteraf kan het zijn dat er nog screening nodig is door het verwisselen van functie of andere civiele baan. Aangezien handhaving achteraf is op basis van de Ambtenarenwet, is dit inefficiënt en administratief belastend. De COID wil een strategische verschuiving. Integriteits- en cyberrisico's moeten worden getransformeerd naar een HR-vraagstuk dat direct bij de werving of een functiewissel, contractueel wordt afgedekt. Deze benadering sluit aan bij de huidige, ingrijpende herziening van het integriteitsbeleid in samenwerking met de Directie Veiligheid. Met een hernieuwde focus op informatiebeveiliging en het voorkomen van fraude en corruptie, vormt dit een meer stimulerende cultuur.

1.2.7 Tussenconclusie

Op basis van het uitgevoerde documentenonderzoek, het observatieonderzoek en het interview kan worden geconcludeerd dat de huidige maatregelen van Defensie om het digitale gedrag van reservisten in hun privétijd en bij hun civiele werkgever te reguleren, vooral uit interne richtlijnen komen, namelijk de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag. In de realiteit houden reservisten zich niet altijd aan deze regels in de privésfeer. Uit het documentenonderzoek is naar voren gekomen dat de Gedragscode Defensie, de Gedragsregels Sociale Veiligheid & Integriteit Defensie en het Handboek Cyberveilig gedrag Defensie duidelijke normen en regels voorschrijven over digitaal gedrag binnen Defensieterrein en het digitaal gedrag in de privésfeer. Echter, alleen de regels in de Gedragscode Defensie en de Gedragsregels Sociale Veiligheid & Integriteit Defensie zijn juridisch afdwingbaar, omdat er ook sancties in staan als deze regels worden overtreden. Het Handboek Cyberveilig gedrag Defensie daarentegen wordt meer als een richtlijn gezien binnen Defensie, er staan geen consequenties in bij het overtreden van deze richtlijn. Wel wordt er geacht dat elke Defensiemedewerker de kennis daarin tot zich opneemt en dat het een randvoorwaarde is bij militaire operaties.

Het observatieonderzoek en het interview laten zien dat 'papieren werkelijkheid' soms botst met het dagelijkse leven van een reservist. Hoewel er een hoog bewustzijn heerst van digitale dreigingen zoals tracking en chantage, kiezen reservisten in de privésfeer soms voor onveilig gedrag als het delen van wifi-netwerken. Er is een verhoogd risico op informatielekken en belangenverstrengeling, doordat reservisten constant schakelen tussen Defensie en hun civiele baan. Uit het observatieonderzoek is naar voren gekomen dat de groep reservisten van beide moreel beraden bewust zijn van de risico's van hun eigen digitale gedrag in de privésfeer. Ze zijn ook bereid om de collectieve belangen boven eigen belangen te zetten als het gaat om veiligheid.

[41] Bijlage 4: Interviewverslag
[42] Bijlage 5: Toestemmingsformulier

© Hogeschool Utrecht, 2026

Ook vinden ze dat stimulering vanuit Defensie als zorg vanuit de werkgever wordt gezien en dit past bij de geadviseerde strategische verschuiving dat de COID wil toepassen.

1.3 De reikwijdte van de interne richtlijnen van Defensie voor reservisten in samenhang met de Wet ambtenaren Defensie

1.3.1 Inleiding

Dit hoofdstuk behandelt deelvraag 2, *"In hoeverre bepalen het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie en de Gedragscode Defensie welke plichten reservisten hebben met betrekking tot hun digitale gedrag binnen hun functie en in hun privéleven en bij hun civiele baan en is dit evenredig gelet op artikel 12a jo. 12bis van de Wet ambtenaren Defensie?"* aan de hand van literatuur en wetgeving. Om deze deelvraag te kunnen beantwoorden moet eerst de rechtspositie van de reservist worden vastgesteld. Op grond van artikel 1 van de Wet ambtenaren Defensie valt een reservist onder de status militair ambtenaar. In paragraaf 3.1.1 wordt er een beeld geschetst van de verschillen tussen een beroepsmilitair en burgermedewerker. Vervolgens wordt in paragraaf 3.1.2 de rechtspositie van een reservist weergegeven. Daarna wordt in paragraaf 3.2 de interne richtlijnen van Defensie behandeld. In paragraaf 3.3 wordt de wettelijke basis toegelicht. Vervolgens wordt in paragraaf 3.4 de grondwet en evenredigheid getoetst. Tot slot wordt de tussenconclusie behandeld in paragraaf 3.5.

Beroepsmilitair en burgermedewerker

Bij Defensie is het personeel onder te verdelen in drie categorieën, waarbij de juridische status verschilt. Het grootste verschil dat centraal staat bij Defensie is het onderscheid tussen het bekleden van een militaire en een niet-militaire functie. Burgermedewerkers vallen juridisch gezien onder een niet-militaire functie. Hierdoor hebben zij ook geen verplichtingen zoals de uitzendplicht of de plicht tot het dragen van een uniform.[43]

In tegenstelling tot de burgermedewerkers vallen beroepsmilitairen en reservisten wel onder een militaire functie. Hierdoor zijn zij onderworpen aan specifieke militaire plichten en het militaire tuchtrecht. Bij Defensie zijn er vier krijgsmachtonderdelen, namelijk de Koninklijke Marine, de Koninklijke Landmacht, de Koninklijke Luchtmacht en de Koninklijke Marechaussee. Daarnaast zijn er ook nog drie Defensieonderdelen, het Defensie Ondersteuningscommando (DOSCO), het Commando Materieel en IT (COMMIT) en de Defensie Bestuursstaf.[44]

Reservist als militair ambtenaar

Hoewel beroepsmilitairen en reservisten een militaire functie hebben, is er wel een cruciaal verschil tussen deze twee groepen, namelijk de hybride positie van een reservist. Een beroepsmilitair heeft een fulltime aanstelling bij Defensie en alleen een privéleven buiten Defensie. Een reservist heeft daarentegen nog een civiele baan en een privéleven buiten Defensie. Dit maakt dat een reservist een unieke rechtspositie heeft, omdat een reservist twee werkgevers heeft. Tijdens de werkelijke dienst is een reservist volledig onderworpen aan Defensie en op andere momenten voert de civiele werkgever het gezag.[45]

Defensie beschouwt de aanstelling reservist als '0-urencontract'. Dit betekent dat afhankelijk van de beschikbaarheid van een reservist er afspraken worden gemaakt met de desbetreffende commandant over hoeveel de reservist wordt ingezet. Dit kan een aantal uren per week of per maand zijn, of per oefening of project.[46] Onafhankelijk van hoeveel uren een reservist daadwerkelijk per jaar voor Defensie werkt, wordt door Defensie de civiele baan als nevenfunctie

[43] 'Burgermedewerker', werkenbijDefensie.nl.
[44] '7 onderdelen 1 Defensie', werkenbijDefensie.nl.
[45] 'Informatie voor werkgevers', werkenbijDefensie.nl.
[46] N. Hummel 2025.

© Hogeschool Utrecht, 2026

aangemerkt. Ook beroepsmilitairen kunnen een nevenfunctie hebben maar dat is dan over het algemeen voor minder uren en niet een baan waarvan hun gezinsinkomen het meest afhankelijk is.[47] Hierin kunnen reservisten dus erg verschillen van beroepsmilitairen, maar er zijn ook reservisten die fulltime voor Defensie werken zonder een civiele baan ernaast. Naast deze verschillen hebben reservisten een overeenkomst met beroepsmilitairen. Zo hebben zij beiden een militaire status. Door deze militaire status vallen reservisten onder het militair strafrecht en het militair tuchtrecht.[48] De periodieke inzetbaarheid en de dubbele binding met de maatschappij van het merendeel van de reservisten zorgen voor een complexer juridisch kader, wat betreft de doorwerking van Defensienormen in de privésfeer en bij de civiele werkgever.

1.3.2 Interne richtlijnen van Defensie

Defensie heeft drie interne kernrichtlijnen om het gedrag van haar personeel aan te sturen, namelijk de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag Defensie. Deze richtlijnen bepalen dat digitale veiligheid een integraal onderdeel is van ‘goed werknemerschap’ en dat deze richtlijnen van toepassing zijn op alle Defensiemedewerkers.

Plichten binnen de militaire functie

Tijdens de dienst bepalen deze richtlijnen de (digitale) plichten van reservisten. De Gedragscode Defensie verplicht reservisten tot het strikt opvolgen van operationele cyberveiligheidsprocedures via de kernwaarden ‘Veiligheid’ en ‘Verantwoordelijkheid’. Deze regels staan toegelicht in de Gedragsregels Defensie Sociale Veiligheid & Integriteit. Het overtreden van deze regels kan leiden tot aangiftes of er wordt mogelijk opgetreden conform de Wet militair tuchtrecht of de (militaire) Ambtenarenwet. Verder vult het Handboek Cyberveilig gedrag Defensie de regels aan met normen voor veilig digitaal gedrag. Algemene voorbeelden hiervan zijn zorgvuldig omgaan met Defensieapparaten en veilig omgaan met social media.

Plichten in het privéleven en de civiele baan

De interne richtlijnen zijn ook van toepassing buiten de kazerne. In de Gedragsregels Defensie Sociale Veiligheid & Integriteit staat dat een medewerker ook in de privétijd en tijdens de uitoefening van een civiele baan aan Defensienormen is gebonden.

Het privéleven van een reservist valt onder het thema ‘*Gedrag in vrije tijd’*. Hierin worden reservisten verplicht om op social media rekening te houden met hoe uitingen invloed kunnen hebben op het imago van Defensie. Een reservist dient personen te vermijden die vaak de wet overtreden. Daarnaast vermijden zij ook situaties die het imago van Defensie kunnen aantasten. Dit is om te voorkomen dat de reservist in een chantabele positie komt.[49]

De civiele baan van een reservist valt onder het thema ‘*Nevenwerkzaamheden’* en *‘Contacten met het bedrijfsleven’*. In dit thema staan in de gedragsregels de plicht om commerciële belangen strikt gescheiden te houden van de Defensierol. Elke schijn van belangenverstrengeling of het lekken van gevoelige (cyber)informatie naar de civiele werkgever is verboden.[50]

1.3.3 De wettelijke basis

Voor het beoordelen of het rechtmatig is dat deze plichten ook in de privésfeer en bij de civiele werkgever gelden, moet worden gekeken naar de wettelijke basis. Op grond van artikel 1 van de Wet ambtenaren Defensie wordt de reservist gezien als militair ambtenaar.[51] Hoewel een

[47] Ministerie van Defensie 2019, p. 19.
[48] N. Hummel & Walgemoed 2016.
[49] Ministerie van Defensie 2019, p. 10-12.
[50] Ministerie van Defensie 2020, p.19-24.
[51] Hummel & Walgemoed 2016.

© Hogeschool Utrecht, 2026

reservist een civiele hoofdbaan heeft, bezit hij een militaire status zodra hij de eed of belofte aflegt.[52] Hierdoor gelden voor de reservist specifieke wettelijke plichten.

Artikel 12a van de Wet ambtenaren Defensie
Op grond van artikel 12a van de Wet ambtenaren Defensie kan het recht op vrijheid van meningsuiting[53] van een reservist worden beperkt, mits de uitoefening van dit recht de goede vervulling van de militaire functie of het goede functioneren van de openbare dienst in gevaar brengt. Er is hier sprake van een wettelijke gezagsverhouding tussen Defensie en reservisten, waarbij Defensie de privacy en meningsuiting van reservisten kan begrenzen.[54]

Artikel 12bis van de Wet ambtenaren Defensie
Een belangrijk wetsartikel is artikel 12bis Wet ambtenaren Defensie. In dit artikel staat dat een reservist de verplichting heeft om zich te gedragen als een *goed militair ambtenaar*. Dit artikel vormt de wettelijke basis voor de interne richtlijnen. De regels in de interne richtlijnen zijn ook hierop gebaseerd en dat is terug te zien in de formulering van de gedragsregels. Een voorbeeld hiervan is te zien in de Gedragscode Defensie. Onder de waarde, vertrouwen, staat "*Ik ben mij altijd bewust van mijn voorbeeldfunctie en de hoge eisen die de samenleving stelt aan mijn gedrag."*

In de Gedragsregels Defensie Sociale Veiligheid & Integriteit staan ook de sancties en de bijbehorende wetgeving. Dit is een 'open norm' die ook gedragingen buiten diensttijd kan omvatten indien deze de belangen van Defensie kan schaden of de betrouwbaarheid van een militair aantast.

1.3.4 Toetsing evenredigheid aan artikel 12a jo. 12bis Wet ambtenaren Defensie

Om te bepalen of een privégedraging de toets van artikel 12a jo. 12bis Wet ambtenaren Defensie doorstaat, kan de casuïstiek worden onderverdeeld in drie categorieën:

1. De gedraging vindt plaats binnen werktijd, maar is privé.
2. De gedraging vindt plaats buiten werktijd, maar heeft een directe relatie met het werk.
3. De gedraging vindt plaats buiten werktijd en heeft op zichzelf niets met het werk te maken, maar de gedraging vindt plaats in een werkgerelateerde situatie.[55]

In dit geval gaat het bij reservisten specifiek om categorie 2 en 3: gedragingen buiten werktijd die een directe relatie hebben met het werk of plaatsvinden in een werkgerelateerde situatie. Bij categorie 2 kan er gedacht worden aan het gebruik van social media en bij categorie 3 kan er gedacht worden aan gedrag bij een personeelsfeest.

<u>Voorbeeld categorie 2</u>
Een reservist plaatst een bericht op Facebook. Op de achtergrond van de foto is zijn Defensieuniform te zien. Dit vindt plaats in de privétijd, maar het heeft wel een directe relatie met Defensie. Uit de foto is namelijk af te leiden dat hij een reservist of militair is.

<u>Voorbeeld categorie 3</u>
Een groep reservisten van een legereenheid organiseren op een zaterdagavond een barbecue bij één van de reservisten thuis. Tijdens de barbecue wordt er alcohol gedronken en één van de

[52] J.A. Pols 2020, p. 6.
[53] Artikel 7 Grondwet
[54] Durve 2001.
[55] Vlot & Arntz 2018.

© Hogeschool Utrecht, 2026

reservisten maakt extreme politieke uitspraken. Dit heeft hij zelf ook gefilmd en op social media geplaatst.

Defensie heeft op grond van artikel 12a jo. 12bis van de Wet ambtenaren Defensie het recht om het recht op vrijheid van meningsuiting van reservisten te beperken als zij door hun (digitale) gedrag zich niet als een goed militair ambtenaar gedragen. Het gaat hierbij om (digitale) gedragingen in de privésfeer of bij de civiele werkgever die de gedragscode van Defensie overschrijden en invloed heeft op het imago of de veiligheid van Defensie.

1.3.5 Tussenconclusie

Het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en de Gedragscode Defensie bepalen in zekere mate welke plichten reservisten hebben. Door hun wettelijke status als militair ambtenaar strekken deze plichten zich rechtmatig uit tot hun privéleven en hun civiele baan, mits hun digitale gedrag een directe impact heeft op de operationele veiligheid of de reputatie van Defensie. Zij horen namelijk als een goed militair ambtenaar te gedragen, ongeacht of het op Defensieterrein of in de privésfeer of bij de civiele werkgever is. Dit staat ook in de Gedragscode waarvoor zij een eed of belofte hebben afgelegd.

1.4 Juridische kwalificatie en afdwingbaarheid van digitale gedragsnormen

1.4.1 Inleiding

Dit hoofdstuk behandelt deelvraag 3, *"In hoeverre kunnen het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en de Gedragscode Defensie als een dienstvoorschrift worden gezien in de zin van artikel 135 van het Wetboek van Militair Strafrecht jo. artikel 18 van de Wet militair tuchtrecht, en gelden de gedragsnormen hierin voor reservisten zowel tijdens hun dienst als in hun privéleven en bij hun civiele baan gelet op artikel 10 van de Nederlandse Grondwet?"* aan de hand van literatuur en wetgeving. In paragraaf 4.1.1 wordt de definitie van een dienstvoorschrift toegelicht. Daarna wordt de toetsing van het Handboek Cyberveilig gedrag Defensie, de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit behandeld in paragraaf 4.2. Vervolgens wordt de reikwijdte in het privéleven en de civiele baan toegelicht in paragraaf 4.3. Tot slot wordt de tussenconclusie in paragraaf 4.4 behandeld.

1.4.2 Definitie dienstvoorschrift

Om deelvraag 3 te kunnen beantwoorden moet er gekeken worden naar de definitie van een dienstvoorschrift, om te kijken of de interne richtlijnen als een dienstvoorschrift kunnen worden gekwalificeerd. Op grond van artikel 135 van het Wetboek van Militair Strafrecht wordt een dienstvoorschrift gedefinieerd als een door het bevoegde gezag vastgestelde algemene regeling die betrekking heeft op de dienst.

Volgens een artikel in het tijdschrift *Militair tuchtrecht* moet een regeling voldoen aan cumulatieve eisen om als dienstvoorschrift te worden aangemerkt. Als eerste moet er sprake zijn van een schriftelijk besluit van een algemene strekking. Daarnaast moet het voorschrift zijn gegeven bij of krachtens algemene maatregel van rijksbestuur of van bestuur dan wel bij of krachtens landsverordening onderscheidenlijk landsbesluit. Dit betekent dat het voorschrift officieel moet zijn vastgelegd in één van de wettelijke documenten van de overheid. Wie deze dienstvoorschriften mag vaststellen is geregeld in artikel 9 lid 2 van het Rijksbesluit uitvoeringsbepalingen militair straf- en tuchtrecht, namelijk de Minister van Defensie, de door de Minister van Defensie aangewezen functionarissen en de bevelvoerend militair. In de derde plaats moet het voorschrift enig militair dienstbelang betreffen, met dienstbelang wordt dienstaangelegenheid bedoeld. Ook moet het voorschrift gericht zijn tot militairen, maar dit hoeft niet uitsluitend gericht te zijn tot

© Hogeschool Utrecht, 2026

militairen. Tot slot moet het voorschrift een gebod of verbod bevatten. Hierbij geldt dat een instructienorm of een taakaanwijzing niet voldoen aan de gebod of verbod eis.[56]

Het niet opvolgen van een dienstvoorschrift kan leiden tot tuchtrechtelijke sancties op grond van artikel 18 van de Wet militair tuchtrecht of een strafrechtelijke vervolging op grond van artikel 137 lid 1 van het Wetboek van Militair Strafrecht.

1.4.3 Toetsing van het Handboek Cyberveilig gedrag Defensie, de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit

Zoals in artikel 135 van het Wetboek van Militair Strafrecht staat geschreven moet er aan vijf voorwaarden worden voldaan om als dienstvoorschrift te worden gekwalificeerd.

Criteria:

1. Schriftelijk besluit van een algemene strekking
2. Bevoegd gezag
3. Militair dienstbelang
4. Gericht tot militairen
5. Bevat een gebod of verbod

Het Handboek Cyberveilig gedrag Defensie

Door te kijken naar de criteria kan worden bepaald of het Handboek Cyberveilig gedrag Defensie kan worden aangemerkt als een dienstvoorschrift. Ten eerste is het een schriftelijk besluit van een algemene strekking. Het is uitgegeven door de Commandant Defensie Cyber Commando. Verder is het ook van militair dienstbelang, want het cybergedrag met de gezamenlijke normen en waarden behoort tot een randvoorwaarde voor militaire operaties. Ook is het handboek gericht op militairen, maar ook op andere Defensiemedewerkers. Tot slot staat er ook een gebod in. De vraag is of de geboden en verboden die erin staan ook zo concreet geformuleerd zijn dat ze voldoen aan deze eis. Dit is te vergelijken met de uitspraak van de Rechtbank Gelderland van 29 december 2020.[57] In deze uitspraak werden de toenmalige duikveiligheidsvoorschriften niet aangemerkt als dienstvoorschrift, wat leidde tot vrijspraak van de betrokken onderofficieren. Dit toont aan dat ethische richtlijnen of te vaag geformuleerde gedragscodes, de juridische toets van artikel 135 van het Wetboek van Militair Strafrecht niet doorstaan.

De Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit

In de uitspraak van de Rechtbank Gelderland van 5 september 2022[58] heeft de rechter geoordeeld dat het *Handboek Militair* als een dienstvoorschrift kan worden aangemerkt. Hoewel de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit aan de eerste vier criteria voldoen, is de vraag of het aan het laatste criterium voldoet. De Gedragscode Defensie bevat basiswaarden. Het bevat geen geboden of verboden en het is ook niet specifiek gericht op het militair dienstbelang. Dit geldt ook voor de Gedragsregels Defensie Sociale Veiligheid & Integriteit. Hierin staan de gedragsregels als richtlijnen hoe Defensiepersoneel zich hoort te gedragen.

De reikwijdte van de instructiebevoegdheid in het privéleven en de civiele baan

Het aantal reservisten bij Defensie blijft groeien, waardoor er een transitie is naar een ‘Adaptieve Krijgsmacht’. Dit heeft geleid tot een veranderend reservistenbeleid.[59] Reservisten

[56] Ammeraal & Van Hoek 2018.
[57] Rb. Gelderland 29 december 2020, ECLI:NL:RBGEL:2020:7081.
[58] Rb. Gelderland 5 september 2022, ECLI:NL:RBGEL:2022:5369.
[59] Sterie 2019.

© Hogeschool Utrecht, 2026

vervullen een unieke dubbelrol: zij zijn tijdelijk in actieve dienst, maar functioneren het grootste deel van de tijd als burger in de civiele maatschappij.

De wettelijke basis voor de plicht van een reservist staat in artikel 12bis van de Wet ambtenaren Defensie. Voor reservisten geldt dat zij zich als 'goed militair ambtenaar' horen te gedragen. Dit is een open norm die geldt tijdens de perioden dat zij in werkelijke dienst zijn. Echter, deze norm geldt ook voor reservisten in hun privéleven en bij hun civiele baan. Hierdoor is de daaraan gekoppelde tuchtrechtelijke en strafrechtelijke aansprakelijkheid van kracht tijdens de periodes dat zij in werkelijke dienst zijn, maar ook buiten hun dienst. Zo kunnen reservisten op grond van artikel 39 lid 2 sub l van het Algemeen militair ambtenarenreglement worden ontslagen wegens wangedrag tijdens de dienst of buiten de dienst voor zover dit gedrag schadelijk is voor de dienstvervulling of niet in overeenstemming is met het aanzien van het ambt.

De noodzaak voor het reguleren van digitaal gedrag
De noodzaak om digitaal gedrag in de privésfeer te reguleren is duidelijker naar voren gekomen om de veiligheid van Defensie te waarborgen. Een voorbeeld hiervan is het gebruik van de app Strava door Defensiepersoneel. Strava is een sportapp waarmee de gebruiker zijn prestaties kan bijhouden. Militairen hebben deze app gebruikt op militaire bases en hierdoor waren in een paar klikken hun profielfoto en woonplaats te vinden.[60] Dit heeft geleid tot het risico dat de operationele veiligheid en persoonlijke veiligheid van Nederlandse militairen in gevaar komen doordat de militairen te traceren zijn. De Staatssecretaris van Defensie heeft in de schriftelijke antwoorden verduidelijkt dat het uploaden van hardloop- of fietsroutes door militairen in hun privétijd de operationele veiligheid in gevaar kan brengen, omdat hierdoor locatiedata van gevoelige militaire locaties of operationele patronen in handen van derden kunnen vallen.[61]

Uit deze casus en aanvullend onderzoek naar digitale veiligheid binnen Defensie blijkt dat digitaal gedrag in de privésfeer direct invloed kan hebben op de operationele veiligheid en de integriteit van de krijgsmacht.[6263] Defensie wil zich inzetten tegen cyberdreigingen.[64] Om dit te kunnen, is het belangrijk dat Defensie en al haar personeel cyberveilig gedrag vertoont. Dit betekent dat Defensie een gerechtvaardigd belang heeft om bepaalde gedragingen in de privésfeer te normeren. Defensie heeft ook regels opgesteld voor de interactie met de buitenwereld die expliciet gelden voor zowel beroepsmilitairen als reservisten.[65] Er is wel een verschil in de juridische handhaafbaarheid. Tijdens de werkelijke dienst gelden alle dienstvoorschriften en cyberveiligheidsnormen. Ze zijn dan volledig afdwingbaar via het Wetboek van Militair Strafrecht en de Wet militair tuchtrecht. Wanneer reservisten zich in hun privéleven of bij hun civiele baan bevinden, kunnen zij niet in de regel van het Wetboek van Militair Strafrecht of de Wet militair tuchtrecht vervolgd worden voor enkel het niet naleven van een gedragsregel die in de richtlijnen staat. Tenzij dat specifieke gedrag een directe en substantiële bedreiging vormt voor de veiligheid van de staat, de operationele veiligheid van Defensie, of de militaire orde.

Het criterium is hier de merkbare impact op de veiligheid van Defensie. Als een reservist in zijn civiele baan of privéleven door onveilig digitaal gedrag, bijvoorbeeld het lekken van Defensiedata, de operationele veiligheid schaadt, kan hij via de algemene norm van het 'goed militair ambtenaarschap[66] of via het Wetboek van Militair Strafrecht aansprakelijk worden gesteld. Echter, reservisten die onveilig digitaal gedrag tonen dat tegen een richtlijn ingaat, maar geen

[60] 'Ruim duizend militairen te traceren via Strava: 'Vijand kan data misbruiken', nos.nl, 19 maart 2025.
[61] *Aanhangsel Handelingen II* 2024/25, nr. 2134.
[62] Ducheine, Pijpers & Zwanenburg 2024, p.9.
[63] *Kamerstukken II* 2024/25, 33763, nr. 158.
[64] *Kamerstukken II* 2025/26, 26643, nr. 1422.
[65] Aanwijzing SG A/978.
[66] Artikel 12a Wet ambtenaar Defensie.

© Hogeschool Utrecht, 2026

schade brengt aan Defensie kan wegens het recht op eerbiediging van de persoonlijke levenssfeer buiten de dienstplichtperiode niet zomaar juridisch worden afgedwongen. Defensie heeft namelijk geen zeggenschap over privéapparatuur en het privégebruik van het internet.[67]

1.4.5 Tussenconclusie

Het Handboek Cyberveilig gedrag Defensie, de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit voldoen niet aan de eisen van artikel 135 van het Wetboek van Militair Strafrecht. Hierdoor vallen ze formeel gezien niet onder een dienstvoorschrift. Deze richtlijnen kennen een dualistisch karakter dat strikt afhankelijk is van de formele status van het document én de actuele status van de reservist. Echter, reservisten zijn wel gebonden aan artikel 12a van de Wet ambtenaren Defensie, waardoor zij zich als 'goed militair ambtenaar' horen te gedragen. Defensie kan een reservist alleen vervolgen op grond van het Wetboek van Militair Strafrecht, wanneer het digitale gedrag van de reservist in zijn privétijd of bij de civiele werkgever de operationele veiligheid van Defensie schaadt, een bedreiging vormt voor de veiligheid van de staat of de militaire orde. Als dit gedrag zowel onder het Wetboek van Militair Strafrecht als onder de Wet militair tuchtrecht valt, dan is in beginsel de commandant niet bevoegd om tuchtrechtelijk op te treden. Deze bevoegdheid ligt bij de strafrechter met uitzondering van de artikelen 6 tot en met 40 van de Wet militair tuchtrecht.[68]

1.5 De toetsingskaders uit de jurisprudentie voor de beperking van gedrag in de privésfeer

1.5.1 Inleiding

Dit hoofdstuk behandelt aan de hand jurisprudentie deelvraag 4, *"In hoeverre mag Defensie het gedrag van reservisten in hun privéleven en bij hun civiele baan beperken op grond van jurisprudentie ten behoeve van de veiligheid van Defensie?".* Dit houdt in dat er wordt gekeken naar relevante jurisprudentie over het gedrag van een werknemer in de privésfeer. Dit is van belang om te weten welke toetsingskaders rechters gebruiken om te beoordelen of een werkgever het gedrag van een werknemer mag beperken in de privésfeer. Hierbij is het van belang om te kijken welke afwegingen rechters maken als het gaat om de schending van het recht op privacy van een werknemer, namelijk het recht op eerbiediging van de persoonlijke levenssfeer. In paragraaf 5.2 wordt het wettelijk fundament uitgelegd. Vervolgens wordt in paragraaf 5.3 het toetsingskader uit de jurisprudentie behandeld. Paragraaf 5.4 gaat over de veiligheid van Defensie en de Verklaring Geen Bezwaar. Daarna wordt in paragraaf 5.5 Integriteitsbeleid, Gedragscodes en Misbruik van de Militaire Status behandeld. Tot slot volgt de tussenconclusie in paragraaf 5.6.

1.5.2 Wettelijke fundament

De rechtspositie van reservisten rust op een formele basis, namelijk de wetgeving. In dit geval wordt er gekeken naar artikel 7, 10 en 109 van de Grondwet. Dit heeft direct invloed op de mate waarin hun vrijheden kunnen worden beperkt.

Artikel 109 van de Grondwet

Artikel 109 van de Grondwet bepaalt dat de wet de rechtspositie, de arbeidsbescherming en de medezeggenschap van alle ambtenaren regelt. Dit legaliteitsbeginsel regelt dat elke beperking die Defensie oplegt aan haar personeel, waaronder ook de reservisten, moet kunnen worden teruggevoerd op een formele wettelijke grondslag.

Artikel 7 en 10 van de Grondwet

Deze artikelen waarborgen de vrijheid van meningsuiting en het recht op eerbiediging van de persoonlijke levenssfeer, oftewel privacy. In de basis geldt dat een reservist net als iedere

[67] *Aanhangsel Handelingen II* 2024/25, nr. 2160.
[68] Ministerie van Defensie 2004, 1410.

© Hogeschool Utrecht, 2026

andere Nederlandse burger recht heeft op privacy en vrijheid van meningsuiting. Echter, deze grondrechten zijn niet absoluut. Dit betekent dat deze rechten bij of krachtens de wet beperkt kunnen worden.

1.5.3 Het toetsingskader uit de jurisprudentie

Wanneer gedragingen van een reservist in de privésfeer of bij de civiele werkgever raken aan de belangen van Defensie, kan Defensie overgaan tot disciplinaire sanctionering, zoals een officiële waarschuwing, schorsing als strafmaatregel of ontslag op staande voet. Daarnaast kunnen ze ook rechtspositionele maatregelen nemen, zoals vrijstelling van werk, overplaatsing of reorganisatie. De rechter toetst dergelijke besluiten aan de hand van een kader waarin de beginselen van goed werkgeverschap centraal staan.

Toerekenbaarheid en evenredigheid

In de uitspraak van de rechtbank Den Haag 20 mei 2022 heeft de rechtbank uiteengezet hoe de rechter de rechtmatigheid van een opgelegde sanctie beoordeelt. De rechter hanteert hierbij een drieledige toets:[69]

1. Toerekenbaarheid: Kan het wangedrag in de privésfeer de medewerker redelijkerwijs worden aangerekend?
2. Evenredigheid: De opgelegde straf of maatregel vanuit Defensie moet in een gezonde en redelijke verhouding staan tot de ernst van het verweten wangedrag. Een te zware sanctie voor een relatief klein privévergrijp houdt in rechte geen stand.
3. Goed werkgeverschap: Defensie dient als overheidswerkgever zorgvuldig te handelen, de feiten objectief vast te stellen en de belangen van de medewerker mee te wegen.

Imagoschade en plichtsverzuim buiten diensttijd

Een belangrijk criterium voor de rechter om te bepalen of privégedrag de werksfeer raakt, is de mate van reputatie- of imagoschade voor de organisatie. In de uitspraak van de Centrale Raad van Beroep van 23 november 2017[70] werd een Defensiemedewerker geconfronteerd met een disciplinaire verplaatsing na grensoverschrijdend gedrag in de privésfeer. De Centrale Raad van Beroep oordeelde dat gedragingen in de privésfeer als 'plichtsverzuim' kunnen worden aangemerkt indien deze gedragingen direct reflecteren op de organisatie en leiden tot imagoschade. De status van Defensie vereist dat medewerkers zich onthouden van gedrag dat het vertrouwen van de samenleving en de politiek in de krijgsmacht ernstig ondermijnt.

Dit principe wordt verder bekrachtigd in de uitspraak van de Centrale Raad van Beroep van 27 augustus 2015.[71] Hier boog de Raad zich over de vraag wanneer wangedrag in de privésfeer ernstig genoeg is om tot de zwaarste sanctie, namelijk ontslag, over te gaan. De jurisprudentie laat zien dat de grens tussen privé en werk vervaagt naarmate het gedrag de integriteit van de medewerker zodanig aantast dat handhaving in de militaire functie onaanvaardbaar is geworden.

1.5.4 Het Bărbulescu-kader

Naast het toetsingskader voor de gedragingen van een reservist in de privésfeer of bij de civiele werkgever is er ook een toetsingskader voor Defensie. Er is een harde grens voor evenredigheid wanneer Defensie overgaat tot actieve controle of monitoring van het digitaal gedrag van reservisten in de privésfeer of bij de civiele werkgever.[72] Het Europees Hof voor de Rechten van de Mens (EHRM) heeft in de arresten Bărbulescu 2017 en de Nederlandse uitwerking daarvan,

[69] Rb. Den Haag 20 mei 2022, ECLI:NL:RBDHA:2022:11509.
[70] CRvB. 23 november 2017, ECLI:NL:CRVB:2017:4066.
[71] CRvB. 27 augustus 2015, ECLI:NL:CRVB:2015:2901.
[72] Tijdschriftschrift Computerrecht 2022.

© Hogeschool Utrecht, 2026

Hof Arnhem-Leeuwarden 2022, strikte criteria opgesteld voor de monitoring van digitaal gedrag:[73]

5. Voorafgaande informatie: Is de werknemer duidelijk geïnformeerd over monitoring?
6. Legitieme grond: Is er een zwaarwegend (veiligheids)belang?
7. Proportionaliteit en subsidiariteit: Kan het doel niet met minder ingrijpende middelen worden bereikt? Is de inbreuk in verhouding tot het risico?
8. Adequate waarborgen: Is er bescherming tegen misbruik van de gegevens?

Bij het toepassen van deze criteria op reservisten, ontstaat er een frictie tussen beleid en de evenredigheid.[74] Een reservist brengt het grootste deel van zijn tijd door in de civiele maatschappij en actieve controle door Defensie op zijn privéapparatuur, privéwachtwoorden of internetgedrag thuis vormt een disproportionele inbreuk op artikel 10 van de Grondwet, namelijk het recht op eerbiediging van de persoonlijke levenssfeer.[75] Er is in de privésfeer geen sprake van een sluitend Defensienetwerk waar monitoring automatisch is toegestaan.[76] Een dwingende controlecultuur in de privésfeer of bij de civiele werkgever schendt de criteria subsidiariteit, als het doel ook via minder ingrijpende middelen kan worden bereikt.

1.5.5 Veiligheid van Defensie en de Verklaring Geen Bezwaar (VGB)

Naast disciplinaire straffen wegens plichtsverzuim, beschikt Defensie over een preventief en zeer ingrijpend instrument: het veiligheidsonderzoek op grond van de Wet veiligheidsonderzoeken. Omdat militaire functies en de meeste reservistenfuncties vertrouwensfuncties zijn, is een geldige Verklaring Geen Bezwaar (VGB) een harde aanstellingsvereiste.

In de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 11 oktober 2023 werd de VGB van een militair ingetrokken vanwege diens gedragingen en dubieuze contacten in de privésfeer.[77] De militair stelde dat deze intrekking een onrechtmatige inbreuk vormde op zijn persoonlijke levenssfeer en zijn vrijheid van vereniging. De Afdeling Bestuursrechtspraak van de Raad van State oordeelde echter dat:
De minister van Defensie heeft een brede beoordelingsruimte om te bepalen of bepaalde privécontacten of gedragingen een risico vormen voor de nationale veiligheid of de veiligheid van de krijgsmacht, zoals het risico op chantage, lekken van informatie of belangenverstrengeling. Het belang van de veiligheid van de staat en de krijgsmacht weegt zwaarder dan de individuele grondrechten van de werknemer. Als het besluit om de Verklaring Geen Bezwaar in te trekken niet onevenredig is, blijft het besluit in stand. Voor een reservist betekent het verlies van de Verklaring Geen Bezwaar direct het einde van de aanstelling.

1.5.6 Integriteitsbeleid

Defensie voert een streng integriteitsbeleid dat nader wordt gespecificeerd in de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit. Dit beleid stelt normen die uitdrukkelijk ook gelden wanneer de medewerker niet in uniform of buiten diensttijd (in de privésfeer of bij de civiele werkgever) handelt.

In de uitspraak van de Centrale Raad van Beroep van 21 oktober 2021 werd het ontslag van een militair wegens wangedrag door de rechter in stand gelaten.[78] De Centrale Raad van Beroep bevestigde dat structurele of ernstige schending van het interne integriteitsbeleid, de

[73] EHRM 5 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608.
[74] Peters 2021.
[75] De laat 2019.
[76] Damen & Baijens 2022.
[77] ABRvS 11 oktober 2023, ECLI:NL:RVS:2023:3762.
[78] CRvB 21 oktober 2021, ECLI:NL:CRVB:2021:2602.

© Hogeschool Utrecht, 2026

Gedragscode, de interne cohesie en de betrouwbaarheid van de organisatie direct schaadt. Van Defensiepersoneel mag wegens de aard van hun taak een verhoogd moreel kompas worden verwacht, ook buiten werktijd.

Een specifiek risico voor reservisten ligt op het snijvlak van hun civiele activiteiten en hun militaire status. In de uitspraak van de rechtbank Zeeland-West-Brabant 20 november 2017 werd geoordeeld over een medewerker die zijn Defensie-e-mailaccount had gebruikt om substantieel financieel voordeel te verkrijgen bij de aanschaf van een auto voor privégebruik.[79] De rechtbank oordeelde dat dit misbruik van de hoedanigheid als Defensiemedewerker ten behoeve van privédoeleinden een duidelijke vorm van plichtsverzuim oplevert. Defensie is bevoegd om het oneigenlijk gebruik van haar naam, status of middelen in de civiele context (zoals ij een civiele baan of in de privésfeer) strikt te reguleren en te sanctioneren.

1.5.7 Tussenconclusie

Er kan geconcludeerd worden dat Defensie op grond van de jurisprudentie wel degelijk beperkingen mag opleggen aan het gedrag van reservisten in het privéleven en bij de civiele baan, mits er een direct of indirect causaal verband bestaat met de veiligheid, integriteit of reputatie van de organisatie. De bevoegdheid om in te grijpen is echter niet onbegrensd. De rechter dwingt Defensie tot het hanteren van een strikte proportionaliteitstoets. Elke rechtspositionele maatregel moet aantoonbaar evenredig zijn aan de ernst van de gedraging en zijn gebaseerd op een zorgvuldige belangenafweging waarbij het beginsel van goed werkgeverschap te allen tijde wordt gerespecteerd. Daarnaast moet er ook aan de criteria van het Bărbulescu-arrest worden gehouden. Dit betekent dat naarmate het risico voor de veiligheid of de integriteit van Defensie concreter is, de ruimte voor de reservist om zich op zijn grondrechten te beroepen, evenredig afneemt.

1.6 Eindconclusie

Voor het adviesrapport is er praktijkonderzoek en onderzoek naar het recht gedaan om de centrale vraag "*In hoeverre mag Defensie het digitale gedrag van reservisten in hun privéleven en bij hun civiele baan beperken op grond van het Handboek Cyberveilig gedrag Defensie, Gedragsregels Defensie, artikel 12a jo. 12bis van de Wet ambtenaren Defensie, artikel 18 van de Wet militair tuchtrecht en jurisprudentie gelet op de bescherming van de persoonlijke levenssfeer op grond van artikel 10 van de Nederlandse Grondwet, met het doel om de veiligheid van Defensie te waarborgen?"* te kunnen beantwoorden. Aan de hand van de deelvragen kan er een onderbouwend antwoord worden gegeven op de centrale vraag.

Deelvraag 1: *"Welke maatregelen neemt Defensie nu om het digitaal gedrag van reservisten veilig te laten verlopen in hun privéleven en bij hun civiele baan ten behoeve van de veiligheid van Defensie?"*. Hierbij is naar voren gekomen dat het huidig beleid van Defensie bestaat uit de Gedragscode Defensie, de Gedragsregels Defensie Sociale Veiligheid & Integriteit en het Handboek Cyberveilig gedrag Defensie. Dit zijn richtlijnen, waarbij alleen de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit het meest bindend is. Verder is er uit het observatieonderzoek naar voren gekomen dat in de praktijk deze gedragsregels niet altijd worden nageleefd, ondanks het feit dat reservisten bewust zijn van de digitale dreigingen.

Deelvraag 2: *"In hoeverre bepalen het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie en de Gedragscode Defensie welke plichten reservisten hebben met betrekking tot hun digitale gedrag binnen hun functie en in hun privéleven en bij hun civiele baan en is dit evenredig gelet op artikel 12a jo. 12bis van de Wet ambtenaren Defensie?"*. Hieruit is naar voren gekomen dat het Handboek Cyberveilig gedrag Defensie, de Gedragsregels Defensie

[79] Rb. Zeeland-West-Brabant 20 november 2017, ECLI:NL:RBZWB:2017:7595.

© Hogeschool Utrecht, 2026

Sociale Veiligheid & Integriteit en de Gedragscode Defensie in mate bepalen welke plichten reservisten hebben. Door hun wettelijke status als militair ambtenaar strekken deze plichten zich rechtmatig uit tot hun privéleven en hun civiele baan, mits hun digitale gedrag een directe impact heeft op de operationele veiligheid of de reputatie van Defensie. Zij horen namelijk als een goed militair ambtenaar te dragen, ongeacht of het op Defensieterrein of in de privésfeer of bij de civiele werkgever is.

Deelvraag 3: *"In hoeverre kunnen het Handboek Cyberveilig gedrag Defensie, Gedragsregels Defensie en Gedragscode Defensie als een dienstvoorschrift worden gezien in de zin van artikel 135 van het Wetboek van Militair Strafrecht jo. artikel 18 van de Wet militair tuchtrecht en gelden de gedragsnormen hierin voor reservisten zowel tijdens hun dienst als in hun privéleven en bij hun civiele baan gelet op artikel 10 van de Nederlandse Grondwet?"*. Het antwoord op deze deelvraag is dat het Handboek Cyberveilig gedrag Defensie, de Gedragscode Defensie en de Gedragsregels Defensie Sociale Veiligheid & Integriteit niet voldoen aan de eisen van artikel 135 van het Wetboek van Militair Strafrecht om als dienstvoorschrift te worden aangemerkt. Deze richtlijnen kennen een dualistisch karakter dat strikt afhankelijk is van de formele status van het document én de actuele status van de reservist. Echter, reservisten zijn wel gebonden aan artikel 12a Wet ambtenaren Defensie, waardoor zij zich als 'goed militair ambtenaar' horen te gedragen. Defensie kan een reservist alleen vervolgen op grond van het Wetboek van Militair Strafrecht, wanneer het digitaal gedrag van de reservist in zijn privétijd of bij de civiele werkgever de operationele veiligheid van Defensie schaadt, een bedreiging vormt voor de veiligheid van de staat of de militaire orde.

Deelvraag 4: *"In hoeverre mag Defensie het gedrag van reservisten in hun privéleven en bij hun civiele baan beperken op grond van jurisprudentie ten behoeve van de veiligheid van Defensie?"*. Hieruit kan er geconcludeerd worden dat Defensie op grond van de jurisprudentie wel degelijk beperkingen mag opleggen aan het gedrag van reservisten in hun privéleven en bij hun civiele baan, mits er een direct of indirect causaal verband bestaat met de veiligheid, integriteit of reputatie van de organisatie. De rechter dwingt Defensie tot het hanteren van een strikte proportionaliteitstoets en elke rechtspositionele maatregel moet aantoonbaar evenredig zijn aan de ernst van de gedraging en zijn gebaseerd op een zorgvuldige belangenafweging waarbij het beginsel van goed werkgeverschap te allen tijde wordt gerespecteerd. Daarnaast moet er ook aan de criteria van de Bărbulescu arrest worden gehouden. Dit betekent dat naarmate het risico voor de veiligheid of de integriteit van Defensie concreter is, de ruimte voor de reservist om zich op zijn grondrechten te beroepen, evenredig afneemt.

Op basis van het uitgevoerde praktijkonderzoek en het onderzoek van het recht kan de centrale vraag beantwoord worden. Defensie mag het digitale gedrag van reservisten in hun privéleven en bij hun civiele baan in beperkte mate reguleren als er wordt voldaan aan het toetsingskader van de rechter. Deze beperking is rechtmatig en evenredig op grond van artikel 12a jo. 12bis Wet ambtenaren Defensie, mits het digitale gedrag van de reservist een directe of indirecte impact heeft op de operationele veiligheid, integriteit of reputatie van de krijgsmacht. Een proactieve controle of monitoring van het digitaal gedrag van reservisten is daarentegen onevenredig en in strijd met artikel 10 van de Grondwet, het recht op privacy.

Aanbevelingen
Uit het onderzoek is naar voren gekomen dat Defensie een aantal stappen kan zetten om het digitaal gedrag van reservisten veiliger te laten verlopen in de privésfeer of bij de civiele baan. Ten eerste kan Defensie het Handboek Cyberveilig gedrag Defensie onderbrengen bij de Gedragscode Defensie. Door het cyberveilig gedrag wat hierin staat te verbinden aan de Gedragscode Defensie, wordt het digitaal wangedrag van een reservist in de privésfeer of bij de civiele baan aan te merken als directe schending van het 'goed militair ambtenaarschap'. Verder kan

© Hogeschool Utrecht, 2026

Defensie het Handboek Cyberveilig gedrag Defensie meer onder de aandacht van reservisten brengen en de sancties die verbonden zijn aan het overtreden van deze regels concretiseren.

Daarnaast kan Defensie een strategie ontwikkelen waarin wordt vastgelegd dat digitale controle alleen wordt ingezet als de veiligheid van Defensie in het geding komt. Bijvoorbeeld nadat er een concrete en onderbouwde melding van een integriteitsschending of datalek is. Er kan hierbij gebruik worden gemaakt van het beroepsproduct, voor het overzichtelijk maken van de stappen dat Defensie het digitaal gedrag van een reservist mag reguleren.

Tot slot is het uitermate belangrijk dat Defensie de reservisten actief ondersteunt door de benodigde faciliteiten beschikbaar te stellen. Zonder die middelen is gewenst digitaal gedrag vertonen onmogelijk. Daarnaast geeft Defensie trainingen aan reservisten over cyberveilig gedrag en hen hierbij begeleidt door bijvoorbeeld het beschikbaar stellen van een wachtwoordmanager.

1.7 Literatuur Juridisch onderzoek

J.C.A. Aarts & M.D. Fink 2025
J.C.A. Aarts & M.D. Fink, *Beschikbaarheid en inzet van burgerambtenaren bij Defensie in tijden van oplopende spanningen*, Den Haag: Ministerie van Defensie, 3 oktober 2025.
- https://puc.overheid.nl/doc/PUC_802201_11/1

D. Ammeraal & J.J.M. van Hoek 2018
D. Ammeraal & J.J.M. van Hoek, 'Het begrip dienstvoorschrift', *Militair straf- en tuchtrecht*, SSR nr. 47, 2019/9.2.
- https://www.inview.nl/document/id72c9415c50ec4eba8fb199083c7977d5/militair-straf-en-tuchtrecht-studiepockets-strafrecht-nr-47-9-2-het-begrip-dienstvoorschrift?ctx=WKNL_CSL_1&tab=tekst&searchid=4094003278

R. Van den Berg
R. Van den Berg, *Handboek Cyberveilig gedrag Defensie,* Den Haag: Ministerie van Defensie (niet openbaar).

E.H. Damen & I. Baijens 2022
E.H. Damen & I. Baijens, 'Monitoring van werknemers: het juridisch kader', *Tijdschrift Arbeidsrecht* 2022/19.
- https://www.inview.nl/document/idc356e1fb4f704c25abcb17c5e65fc055/arbeidsrecht-maandblad-voor-de-praktijk-monitoring-van-werknemers-het-juridisch-kader?ctx=WKNL_CSL_9&tab=tekst&searchid=4094498433

P. Ducheine, P. Pijpers & M. Zwanenburg 2024
P. Ducheine, P. Pijpers & M. Zwanenburg, *Tanden voor de Leeuw,* Breda: Faculteit Militaire Wetenschappen, Nederlandse Defensie Academie 2024.
- https://open.overheid.nl/documenten/e8d9cd92-fe6e-4a6f-a27b-9673649c2643/file

S.A. Durve 2001
S.A. Durve, 'Privacyregelgeving in een nieuwe jas: Little Brother op de werkvloer', *Tijdschrift Arbeidsrecht* 2001/8.
- https://www.inview.nl/document/inod40e15aae48c97d8f603921182bd94735/arbeidsrecht-maandblad-voor-de-praktijk-privacyregelgeving-in-een-nieuwe-jas-little-brother-op-de-werkvloer?ctx=WKNL_CSL_9&tab=tekst&searchid=4091146253

© Hogeschool Utrecht, 2026

N. Hummel 2025
N. Hummel, 'De reservist: twee werkgevers, één missie', *Tijdschrift Recht & Arbeid,* 2025/81.
- https://www.inview.nl/document/idf771dc498ca0411d987440c8c9d37280/tijdschrift-recht-en-arbeid-de-reservist-twee-werkgevers-n-mis-sie?ctx=WKNL_CSL_201&tab=tekst&searchid=4074960284

N. Hummel & Walgemoed 2016
N. Hummel & Walgemoed, 'Beroepsmilitairen en reservisten zijn militair ambtenaar', *Hoofdzaken van het militaire ambtenarenrecht (MM SBR)*, 2016/2.4
- https://www.inview.nl/document/idpass10056ef67a494cfd8aa4fbc6b4fdeb46/hoofdzaken-van-het-militaire-ambtenarenrecht-mastermonografie-n-staats-en-bestuursrecht-2-4-beroepsmilitairen-en-reservisten-zijn-militair-ambte-naar?ctx=WKNL_CSL_1302&tab=tekst&searchid=4091106329

I.J. de Laat 2019
I.J. de Laat, 'Omzien en inzien: een roep om wetgeving over het monitoren van werknemers, alcohol- en drugstesten en het inzagerecht', *Tijdschrift Arbeidsrecht* 2019/33.
- https://www.inview.nl/document/idf645f43fc099414798887d0e0b29174d/arbeidsrecht-maandblad-voor-de-praktijk-omzien-en-inzien-een-roep-om-wetgeving-over-het-monitoren-van-werknemers-alcohol-en-drugstesten-en-het-inzage-recht?ctx=WKNL_CSL_9&tab=tekst&searchid=4094069020

Ministerie van Defensie
Ministerie van Defensie, 'Defensie Cyber Commando', Defensie.nl.
- https://www.Defensie.nl/organisatie/bestuursstaf/cds/Defensie-cyber-commando

Ministerie van Defensie
Ministerie van Defensie, 'Bedreigingen in de digitale omgeving', Defensie.nl.
- https://www.Defensie.nl/onderwerpen/c/cyber/bedreigingen

Ministerie van Defensie 2004
Ministerie van Defensie, *Handleiding militair tuchtrecht*, Den Haag: Ministerie van Defensie, 9 februari 2016.
- https://puc.overheid.nl/doc/PUC_110560000000_10/1

Ministerie van Defensie 2018
Ministerie van Defensie, *Gedragscode Defensie,* Den Haag: Ministerie van Defensie, 4 december 2018.
- https://www.Defensie.nl/site/binaries/site-content/collections/documents/2018/12/04/gedragscode-Defensie/Gedragscode+Defensie.pdf

Ministerie van Defensie 2019
Ministerie van Defensie, *Gedragsregels Defensie Sociale Veiligheid & Integriteit*, Versie 1.0. Den Haag: Ministerie van Defensie 2019 (herzien 1 mei 2020).
- https://www.Defensie.nl/site/binaries/site-content/collections/documents/2020/12/21/gedragsregels-Defensie/Gedragregels+Defensie+Sociale+Veiligheid+en+Integriteit_tcm4-1418035.pdf

Ministerie van Defensie 2025

© Hogeschool Utrecht, 2026

Ministerie van Defensie, *'Defensie Cyberstrategie 2025',* Den Haag: Ministerie van Defensie 2025.
- https://www.Defensie.nl/site/binaries/site-content/collections/documents/2025/10/03/Defensie-cyber-strategie-2025/Defensie+Cyberstrategie+-+openbaar.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Cybersecuritybeeld Nederland 2025', nctv.nl.
- https://www.nctv.nl/onderwerpen/c/cybersecuritybeeld-nederland

S.S.M. Peters 2021
S.S.M. Peters, 'Monitoring en surveillance op het werk – de werknemer opnieuw geknecht?', *Tijdschrift Recht & Arbeid* 2021/42.
- https://www.inview.nl/document/id6f80cb6793c648858d53b3bf8c5afc3f/tijdschrift-recht-en-arbeid-monitoring-en-surveillance-op-het-werk-de-werknemer-opnieuw-geknecht?ctx=WKNL_CSL_201&tab=tekst&searchid=4094057330

J.A. Pols 2020
Ministerie van Defensie, *Brochure rechtspositie reservist algemeen 2020,* Den Haag: Ministerie van Defensie 2020.
- https://www.cmc-Defensie.nl/wp-content/uploads/2021/03/Brochure-rechtspositie-reservist-algemeen-2020.pdf

D. Rountree 2013
D. Rountree, *Federated Identity Primer*, 1e druk, Amsterdam: Elsevier/Syngress 2012, te raadplegen via Sciencedirect.
- https://www.sciencedirect.com/book/monograph/9780124071896/federated-identity-primer

S. Sterie 2019
S. Sterie, *'Gebrekkig reservistenbeleid in de adaptieve krijgsmacht',* Versie 1, Den Haag: Ministerie van Defensie 2019.
- https://puc.overheid.nl/doc/PUC_286125_11/1

Tijdschrift Computerrecht 2022
'Hof bevestigt criteria monitoring e-mailbox werknemer', *Tijdschrift Computerrecht* 2022/202.
- https://www.inview.nl/document/id37d99b6143154e7ab68b51dca2bcd155/computerrecht-hof-bevestigt-criteria-monitoring-e-mailbox-werknemer?ctx=WKNL_CSL_26&tab=tekst&searchid=4094074479

T.J. Vlot & A.H. Arntz 2018
T.J. Vlot & A.H. Arntz, 'Privégedragingen en ontslag', *Tijdschrift ArbeidsRecht* 2018/39.
- https://www.inview.nl/document/idf97bfb43b0cf4b31af245a350ed3d9ce/arbeidsrecht-maandblad-voor-de-praktijk-priv-gedragingen-en-ontslag?ctx=WKNL_CSL_9&tab=tekst&searchid=4091147474

ABRvS 11 oktober 2023, ECLI:NL:RVS:2023:3762.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RVS:2023:3762&showbutton=true&keyword=ECLI%253aNL%253aRVS%253a2023%253a3762.&idx=1

CRvB 23 november 2017, ECLI:NL:CRVB:2017:4066.

© Hogeschool Utrecht, 2026

- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:CRVB:2017:4066&showbutton=true&keyword=ECLI%253aNL%253aCRVB%253a2017%253a4066&idx=1

CRvB 27 augustus 2015, ECLI:NL:CRVB:2015:2901.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:CRVB:2015:2901&showbutton=true&keyword=ECLI%253aNL%253aCRVB%253a2015%253a2901&idx=1

CRvB 21 oktober 2021, ECLI:NL:CRVB:2021:2602.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:CRVB:2021:2602&showbutton=true&keyword=ECLI%253aNL%253aCRVB%253a2021%253a2602&idx=1

EHRM 5 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608.
- https://www.inview.nl/document/id75327cde8c0246fab23529c3e33afa84/njb-2017-1920-art-8-evrm-recht-op-respect-voor-priv-leven-familieleven-en-vertrouwelijke-correspondentie-monitoren-van-elektronisch-berichtenv?ctx=WKNL_CSL_85&anchor=documentgegevens&tab=tekst

Hof Arnhem-Leeuwarden 5 juli 2022, ECLI:NL:GHARL:2022:6203.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHARL:2022:6203&showbutton=true&keyword=ECLI%253aNL%253aGHARL%253a2022%253a6203&idx=1

Rb. Den Haag 20 mei 2022, ECLI:NL:RBDHA:2022:11509.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2022:11509&showbutton=true&keyword=ECLI%253aNL%253aRBDHA%253a2022%253a11509&idx=1

Rb. Gelderland 5 september 2022, ECLI:NL:RBGEL:2022:5369.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBGEL:2022:5369&showbutton=true&keyword=ECLI%253aNL%253aRBGEL%253a2022%253a5369.&idx=1

Rb. Gelderland 29 december 2020, ECLI:NL:RBGEL:2020:7081.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBGEL:2020:7081&showbutton=true&keyword=ECLI%253aNL%253aRBGEL%253a2020%253a7081&idx=1

Rb. Zeeland-West-Brabant 20 november 2017, ECLI:NL:RBZWB:2017:7595.
- https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBZWB:2017:7595&showbutton=true&keyword=ECLI%253aNL%253aRBZWB%253a2017%253a7595&idx=1

Aanhangsel Handelingen II 2024/25, nr. 2134.
- https://zoek.officielebekendmakingen.nl/ah-tk-20242025-2134.pdf

Aanhangsel Handelingen II 2024/25, nr. 2160.
- https://zoek.officielebekendmakingen.nl/ah-tk-20242025-2160.html

Kamerstukken II 2025/26, 26643, nr. 1422.
- https://zoek.officielebekendmakingen.nl/kst-26643-1422.html

Kamerstukken II 2024/25, 33763, nr. 158.
- https://zoek.officielebekendmakingen.nl/kst-33763-158.html

Ministerie van Defensie, *Aanwijzing SG A/978 Extern Optreden, mediacontacten en publicaties,* februari 2020.
- https://zoek.officielebekendmakingen.nl/blg-937337.pdf

© Hogeschool Utrecht, 2026

Bijlage 5: Literatuurlijst

Beuth, P., Diehl, J., Höfner, R., Lehberger, R., Röhreke, F., & Schmid, F. (2025, maart 27). Private Data and Passwords of Senior U.S. Security Officials Found Online. *Der Spiegel*. https://www.spiegel.de/international/world/pete-hegseth-mike-waltz-tulsi-gabbard-private-data-and-passwords-of-senior-u-s-security-officials-found-online-a-14221f90-e5c2-48e5-bc63-10b705521fb7

Carey, R. N., Connell, L. E., Johnston, M., Rothman, A. J., de Bruin, M., Kelly, M. P., & Michie, S. (2019). Behavior Change Techniques and Their Mechanisms of Action: A Synthesis of Links Described in Published Intervention Literature. *Annals of Behavioral Medicine*, *53*(8), 693-707. https://doi.org/10.1093/abm/kay078

Ministerie van Defensie (2026) Kamerbrief stand van zaken maatregelenbrief 'Onze mensen, onze toekomst: meer, beter en sneller'.

Ministerie van Werk en participatie en Ministerie van Defensie (2026), Kamerbrief rechtspositie van de reservist, 3 juli 2026

Schenk, P. M., Wright, A. J., West, R., Hastings, J., Lorencatto, F., Moore, C., Hayes, E., Schneider, V., & Michie, S. (2024). An ontology of mechanisms of action in behaviour change interventions. *Wellcome Open Research*, *8*, 337. https://doi.org/10.12688/wellcomeopenres.19489.1

Van Kessel D, Brommersma B. en Reuver M. (2026) Dankzij lekke reisapp Polarstep weet FTM waar je was deze zomer, Follow the Money 4 september 2026

Vervaart, J. (2025, maart 19). *Persoonsgegevens honderden militairen zichtbaar via sportapp Strava.* Omroep Gelderland. https://www.gld.nl/nieuws/8285161/persoonsgegevens-honderden-militairen-zichtbaar-via-sportapp-strava

© Hogeschool Utrecht, 2026