Rathenau Instituut

Kennis in het vizier

De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur

Rapport

Auteurs
Gijs Diercks, Jasper Deuten & Paul Diederen

Foto omslag
Studenten aan het werk op de campus van de Erasmus Universiteit Rotterdam. Foto: David Rozing / Hollandse Hoogte

Bij voorkeur citeren als:
Diercks, G., J. Deuten en P. Diederen (2019). *Kennis in het vizier – De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur*. Den Haag: Rathenau Instituut

Voorwoord

Huawei is momenteel nauwelijks weg te denken uit het nieuws. De VS roepen op niet met het Chinese telecombedrijf samen te werken, omdat het de Chinese overheid zou faciliteren in cyberspionage. Doordat harde bewijzen hiervoor ontbreken, is het lastig om te onderscheiden welke motieven mogelijk meespelen in een wereld waar economische, politieke en militaire belangen door elkaar lopen. Duidelijk is dat in tijden van verschuivende geopolitieke verhoudingen, kennis en innovatie een machtsmiddel worden.

Dit vraagt om herbezinning op vraagstukken rondom kennisontwikkeling: welke kennis en technologie willen we als Nederland wel of niet ontwikkelen? Met welke partners? En onder welke voorwaarden? In dit rapport verkennen we hoe Nederlandse kennisinstellingen zich op een verantwoorde manier tot de huidige context kunnen verhouden, en wat hierin de rol is van de Nederlandse overheid.

Op basis van interviews en uitgebreid literatuuronderzoek brachten we in beeld hoe sinds de Tweede Wereldoorlog kennis wordt ontwikkeld voor defensie en veiligheid. We concluderen dat de huidige ontwikkelingen gevolgen hebben voor de van oorsprong civiel georiënteerde instellingen: universiteiten, hogescholen en publieke kennisorganisaties. Zij krijgen steeds meer te maken met kennis die militaire toepassingen kan hebben en mogelijk raakt aan nationale veiligheid, zoals robotica en kunstmatige intelligentie (AI).

Dit rapport past in onze onderzoekslijn rond vitale kennisecosystemen, waarin we de toekomstbestendigheid onderzoeken van de manier waarop we kennis voor de samenleving organiseren. Met het huidige onderzoek en eerdere studies, zoals ‘Cyberspace zonder conflict’, willen we bijdragen aan de gedachtevorming over de invloed van technologische ontwikkelingen op in Nederland gekoesterde waarden, in een wereld waarin internationale verhoudingen veranderen.

Wetenschap en technologie hebben inmiddels een belangrijke rol in de Nederlandse Chinastrategie van mei 2019. Het gesprek hierover tussen ministeries en kennisinstellingen is op gang gekomen. Nu is het zaak om op democratische wijze te komen tot nieuwe afwegingskaders en procedures. Dit rapport schetst de voorwaarden voor de invulling daarvan.

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Samenvatting

Een nieuwe wapenwedloop dient zich aan
De geopolitieke verhoudingen in de wereld zijn aan het verschuiven, vooral door de ontwikkeling van de economische en politieke macht van China. In deze nieuwe geopolitieke werkelijkheid staan kennis en innovatie als strategisch machtsmiddel weer hoog op de politieke agenda. Wereldwijd worden nieuwe kennis- en innovatieagenda's geformuleerd om op strategische kennisgebieden een voorsprong te ontwikkelen of te behouden. Bekende voorbeelden zijn de Amerikaanse *Third Offset Strategy,* het Chinese *Made in China 2025* en het nieuwe Defensiefonds van de Europese Unie. Ook in Nederland kwam het ministerie van Defensie in 2018 met een nieuwe Defensie Industrie Strategie, een nieuwe Defensie Cyberstrategie en een nieuwe Innovatiestrategie Defensie.

Met name digitalisering wordt gezien als een bepalende technologische ontwikkeling. Niet alleen kent nieuwe kennis rondom kunstmatige intelligentie en robotica militaire toepassingen. Ook brengt digitalisering van de samenleving een breed spectrum aan dreigingen en kwetsbaarheden met zich mee, van cyberspionage en desinformatie tot sabotage van vitale infrastructuren.

Met deze studie brengen we in kaart wat de belangrijkste gevolgen van die ontwikkelingen zijn voor de Nederlandse publieke kennisinfrastructuur, bestaande uit universiteiten en publieke onderzoeksinstituten. Hiervoor deden we een uitgebreide literatuurstudie, interviewden we deskundigen en voerden een aanvullende casestudy in het maritieme domein uit. Dit laatste omdat Nederland in dat domein van oudsher beschikt over een goede kennisbasis en relatief sterke industrie.

Dit rapport past in onze onderzoekslijn rond vitale kennisecosystemen, waarin we de belangrijkste ontwikkelingen binnen het kennis- en innovatielandschap in kaart brengen. Dit onderzoek is onderdeel van een reeks verkenningen waarin het Rathenau Instituut zich buigt over de implicaties van nieuwe technologische ontwikkelingen voor veiligheid en kwetsbaarheid, in een wereld waarin internationale verhoudingen in rap tempo lijken te verharden. Met dit onderzoek willen we bijdragen aan de gedachtevorming en beleidsdiscussie over de verantwoordelijkheid van publieke kennisinstellingen - ook instellingen met een oorspronkelijk civiele oriëntatie - wat betreft de verdediging van in Nederland gekoesterde waarden.

Verschillen met het verleden
Ook in het verleden werd technologische superioriteit als cruciaal gezien om rivalen voor te blijven. In de wapenwedloop tijdens en na de Tweede Wereldoorlog investeerden overheden in onderzoekscentra en laboratoria voor defensieonderzoek en de ontwikkeling van een eigen defensie-industrie. In vergelijking met die vorige wapenwedloop zien we twee belangrijke ontwikkelingen:

- **Het vervagen van het onderscheid tussen kennisontwikkeling voor civiele en militaire doelen**. Met name digitalisering leidt ertoe dat het onderscheid tussen kennisontwikkeling voor civiele en militaire doelen steeds lastiger te maken is. Bovendien creëren civiele toepassingen van digitale technologieën allerlei nieuwe kwetsbaarheden - denk aan de veiligheidsrisico's rondom het internet der dingen, of de rol van *social media*-platforms in de verspreiding van nepnieuws.
- **Het internationaliseren van kennisontwikkeling en innovatie, in het bijzonder die gericht op defensie en veiligheid**. Kennisontwikkeling vindt steeds meer plaats in internationale samenwerking. Dat geldt ook voor kennisontwikkeling op het gebied van defensie en veiligheid.

Gevolgen voor de publieke kennisinfrastructuur
Deze trends hebben gevolgen voor de publieke kennisinfrastructuur. We maken onderscheid tussen enerzijds de TO2-instellingen (instellingen voor toegepast onderzoek) TNO, MARIN en NLR, die van oudsher een belangrijke rol spelen in militaire kennisecosystemen, en anderzijds de publieke kennisinstellingen die hier niet of nauwelijks onderdeel van waren. Voor de TO2-instellingen met een geschiedenis in militaire kennisontwikkeling blijft de hechte samenwerking tussen overheid, publieke kennisinstellingen en bedrijfsleven – de 'gouden driehoek' – belangrijk. Wel dwingen de trends van digitalisering en internationalisering deze partijen tot: (a) meer en sterkere verbindingen met civiele kennisecosystemen om te kunnen voortbouwen op civiele kennis en technologie; en (b) meer internationale samenwerking, taakverdeling en specialisatie. Meer samenwerking roept de vraag op in hoeverre Nederlandse kennisinstellingen, bekeken vanuit veiligheidsbelangen, kennis zelf in huis moeten hebben en in welke mate ze afhankelijk kunnen zijn van de kennisbasis van binnen- en buitenlandse partners.

De gevolgen van de genoemde trends zijn ingrijpender voor de van oorsprong civiel georiënteerde instellingen: universiteiten, hogescholen, TO2-instellingen en Rijkskennisinstellingen. Door de geschetste ontwikkelingen wordt deze instellingen vaker iets gevraagd dat te maken heeft met defensie- en veiligheid. Dat is reden om de betrokkenheid van de publieke kennisinfrastructuur bij defensie- en veiligheidsvraagstukken opnieuw te doordenken.

We onderscheiden daarbij drie kwesties.

1. Thema's van mogelijk militaire betekenis

Het is belangrijk beleid te ontwikkelen ten aanzien van:

- *Inhoud van het onderzoek.* Als onderzoek (mogelijk) militaire betekenis heeft of leidt tot nieuwe kwetsbaarheden, is er behoefte aan richtlijnen om te bepalen of en onder welke voorwaarden wel of niet in dit onderzoek te participeren.
- *Open science.* Vrij beschikbare data en open communicatie over wetenschappelijk onderzoek kan op gespannen voet staan met veiligheidsbelangen.
- *Fysieke en digitale infrastructuur*. Procedures voor toegang tot laboratoria, computerfaciliteiten en digitale netwerken binnen civiel georiënteerde kennisinstellingen moeten wellicht worden aangescherpt.
- *Wervings- en personeelsbeleid.* De werving van onderzoekers of studenten uit niet-bondgenootlanden creëert mogelijk veiligheidsrisico's.
- *Bronnen van financiering.* Sommige bronnen van financiering kunnen leiden tot ongewenste afhankelijkheden, bijvoorbeeld van buitenlandse overheden of bedrijven met militaire connecties.
- *Internationaliseringsactiviteiten.* Internationale samenwerking met buitenlandse partners kan gepaard gaan met veiligheidsrisico's.

2. Verdeling van verantwoordelijkheden

De verantwoordelijkheid voor het omgaan met de genoemde beleidsvraagstukken is verdeeld over drie niveaus: de politiek, de instelling, en de onderzoeker.

- *Het politieke niveau.* Het is aan de nationale overheid om de kaders vast te stellen waarbinnen kennisinstellingen beleid dienen te formuleren ten aanzien van de zes genoemde aspecten. Veiligheidsbelangen moeten daarvoor worden afgewogen tegen tal van andere belangen. Zoals de belangen van vrije wetenschap, economische ontwikkeling en concurrentiekracht, internationale positie, excellente wetenschap en het aantrekken van kenniswerkers, de aanpak van maatschappelijke uitdagingen en het bijdragen aan *global public goods*. Hierbij speelt de internationale dimensie een belangrijke rol, aangezien veel van deze kaders internationaal en binnen Europa moeten worden afgesproken.

- *Het niveau van de kennisinstellingen.* Het is aan de kennisinstellingen om binnen nationaal vastgestelde kaders verder handen en voeten te geven aan beleid op de zes genoemde aspecten. Daarbij gaat het om de ontwikkeling en implementatie van regels en procedures, om de vaststelling

van professionele gedragscodes en de instelling van organen die zich met veiligheidsaspecten bezighouden.

- *Het niveau van de individuele onderzoeker.* Van individuele onderzoekers mag alertheid worden verwacht: het tijdig aankaarten van zaken met een potentieel veiligheidsrisico - of het nou gaat om de inhoud van het onderzoek, communicatie, samenwerking, financiering of andere aspecten. Het is tevens belangrijk dat onderzoekers hun kennis en zorgen inbrengen in het publieke debat.

3. Benodigde vervolgstappen

Voor biologische, chemische, radiologische en nucleaire kennis en technologie bestaan er al langere tijd *dual-use* arrangementen en is er exportcontrole. Dergelijke arrangementen zijn echter niet ontworpen met het oog op de digitale samenleving, waar veel meer onderzoek *dual-use* is dan vroeger. In de huidige context schiet het toepassen van de regels voor *dual-use* vaak al snel tekort.

De uitdaging is nu om procedures te ontwikkelen die helpen bij het verantwoord omgaan met activiteiten die mogelijk militaire betekenis hebben. Als bron van inspiratie voor de omgang met aspecten van defensie en veiligheid kunnen de procedures dienen die in de loop der tijd zijn ontwikkeld rondom ethische vraagstukken, bestaande wetenschappelijke integriteitscodes of de meer recente gedachtevorming rond het concept *Responsible Research and Innovation*.

De eerste stappen worden gezet. Wetenschap en technologie hebben een belangrijke rol in de Nederlandse Chinastrategie van mei 2019. Het gesprek hierover tussen ministeries en kennisinstellingen is op gang gekomen. Nu is het zaak om te komen tot nieuwe afwegingskaders, heldere procedures en duidelijke afspraken om maatschappelijk verantwoord vorm te geven aan kennisontwikkeling die raakt aan defensie en veiligheid. Hiervoor is gezamenlijk beleid van overheid en kennisinstellingen nodig. Dit rapport schetst daarvan de contouren; nu komt het aan op invulling en uitwerking.

Inhoud

Inleiding

Waar in de eerste 25 jaar na het einde van de Koude Oorlog de machtsverhoudingen min of meer stabiel waren, lijken we nu in een fase van grondige herschikking aanbeland. Met de opkomst van landen als China, Rusland, Indonesië, India, Brazilië en Mexico vindt een verschuiving plaats van zowel economische als politieke macht. Dit vertaalt zich in meer handelspolitieke spanningen, rivaliteit over de toegang tot grondstoffen en transportroutes en uitbreiding van het militaire machtspotentieel. De voorheen als oppermachtig beschouwde positie van de Verenigde Staten als voorloper in de internationale orde wordt bedreigd. Er is geen sprake meer van een '*single global superpower'*, maar er ontstaat een nieuwe wereldorde waarin diverse grootmachten naast elkaar bestaan (WRR, 2018).

Digitalisering als gamechanger

'Wie de leider wordt in kunstmatige intelligentie zal over de wereld heersen', zei de Russische president Poetin in 2017 (van Noort, 2018). Deze quote illustreert dat, in de nieuwe geopolitieke werkelijkheid, kennis en innovatie bovenaan de politieke agenda staan als strategische middelen voor economische en militaire macht. Met name digitalisering wordt gezien als een bepalende technologische ontwikkeling. Ten eerste kent nieuwe kennis rondom kunstmatige intelligentie en robotica ook militaire toepassingen. Denk bijvoorbeeld aan ondersteuning van militairen met behulp van *augmented reality* of de inzet van, potentieel dodelijke, autonome wapensystemen (Ministerie van Defensie, 2016; De Spiegeleire & Sweijs, 2017). Ten tweede wordt 'cyber' met de opkomst van de digitale samenleving vaak gezien als het vijfde domein van conflict, naast land, zee, lucht en ruimte. Dit brengt een breed spectrum aan nieuwe dreigingen mee: van cyberspionage en desinformatie tot sabotage van vitale infrastructuren bij banken of energiebedrijven. Bekende voorbeelden zijn de vermeende sabotage van Iranese kerncentrifuges door de Amerikanen, de beïnvloeding van de Amerikaanse presidentsverkiezingen met behulp van desinformatie door de Russen en diverse beschuldigingen van bedrijfsspionage door de Chinezen (Hamer et al, 2019). Wereldwijd ontvouwt zich een digitale wapenwedloop om koploper te zijn in de ontwikkeling van deze nieuwe technologieën, voor zowel defensieve als offensieve toepassingen. Op mondiale schaal domineren militaire grootmachten zoals de Verenigde Staten, China en Rusland die wapenwedloop, maar ook de Europese Commissie en de Nederlandse overheid ontwikkelen diverse kennis- en innovatieagenda's op dit gebied.

De historische context van kennisontwikkeling voor defensie en veiligheid
Binnen die digitale wapenwedloop wereldwijd worden instellingen uit de publieke kennisinfrastructuur ingezet. Zo worden universiteiten en onderzoeksinstituten in het kader van de technologische race aangespoord en gemobiliseerd om kennis te ontwikkelen voor kennis- en innovatieagenda's, ten behoeve ven defensie en veiligheid. Dit soort mobilisatiestrategieën zijn niet nieuw. Ook in het verleden werden technologische superioriteit en voorsprong in kennis als cruciaal gezien om de tegenstander voor te blijven. Zo veroorzaakte buskruit een revolutie in de middeleeuwse oorlogsvoering in Europa, en stond de Eerste Wereldoorlog in het teken van diverse technologische innovaties – van tanks en vliegdekschepen tot vlammenwerpers en gifgas. Berucht is ook de wapenwedloop tijdens en na de Tweede Wereldoorlog. Deze richtte zich in eerste instantie vooral op kennis over nucleaire fysica en het ontwikkelen van een kernwapenarsenaal, maar breidde zich snel uit. Diverse overheden investeerden in onderzoekscentra en laboratoria voor defensieonderzoek en de ontwikkeling van een eigen defensie-industrie; een combinatie die leidde tot de term *militair-industrieel-wetenschappelijk complex*. Vaak wordt naar de VS verwezen, maar ook de twee Europese 'winnaars' van de Tweede Wereldoorlog, het Verenigd Koninkrijk en Frankrijk, investeerden veel in militaire R&D. Zij bouwden in deze tijd een relatief grote nationale industrie rondom defensie en veiligheid.

Ook in Nederland werd na de Tweede Wereldoorlog doelgericht geïnvesteerd in toegewijde onderzoekscentra en laboratoria voor defensieonderzoek. Voor toegepast defensieonderzoek werd in 1946 de Rijksverdedigingsorganisatie TNO opgericht, de voorloper van het huidige TNO Defensie & Veiligheid (Schippers en Lintsen, 2012). Andere publieke kennisinstituten waar toegepast defensie-onderzoek plaatsvindt, zijn MARIN, NLR, Clingendael en de NLDA (Nederlandse Defensie Academie). Voor meer fundamenteel onderzoek op strategische kennisgebieden werd in 1946 ook FOM opgericht, de stichting voor Fundamenteel Onderzoek der Materie. Alhoewel FOM van begin af aan een exclusief civiele missie meekreeg, kan de belangstelling voor fysisch en nucleair onderzoek in Nederland niet los worden gezien van het vallen van de atoombommen en het brede maatschappelijke en politieke besef dat wetenschap en oorlog nu voorgoed met elkaar verbonden waren (Hoeneveld, 2018). Kenmerkend voor de Nederlandse militaire kennisecosystemen is dat Nederlandse universiteiten een beperkte rol hebben, en onderzoek voor militaire doeleinden door universiteiten in Nederland historisch gezien een gevoelig thema is (Gummet & Stein, 1997; Cops, 2018).

Kennisontwikkeling voor defensie en veiligheid in de digitale samenleving
In deze studie brengen we in beeld wat de overeenkomsten en verschillen zijn tussen de historische en huidige wapenwedloop. We zien dat de huidige context

een andere dynamiek kent in vergelijking met de wapenwedloop tijdens de Koude Oorlog.

Ten eerste zorgt de digitalisering van de samenleving dat civiele kennisontwikkeling een grotere rol speelt dan vroeger. Zo zijn overheden afhankelijk van kennis van universiteiten en bedrijven uit het civiele domein om overwicht te kunnen behouden of te verkrijgen rondom digitale sleuteltechnologieën. Tegelijkertijd creëren deze van oorsprong civiele actoren allerlei kwetsbaarheden op het gebied van defensie en veiligheid, waar zij zich bij voorbaat niet altijd bewust van zijn. Denk bijvoorbeeld aan de veiligheidsrisico's rondom het 'internet der dingen', of de rol van techgiganten in de verspreiding van nepnieuws.

Ten tweede maken de zojuist besproken partijen onderdeel uit van een mondiaal kennisecosysteem. Anders dan de nationaal georganiseerde militaire kennisecosystemen van voorheen, heeft kennisontwikkeling voor defensie en veiligheid in de huidige context een uitgesproken internationaal karakter. Voor een klein en open land als Nederland biedt dit veel kansen; dit wordt bijvoorbeeld zichtbaar in de succesvolle deelname van TNO aan nieuwe Europese onderzoeksprogramma's rondom het thema veiligheid. Tegelijkertijd zien we dat de eerdergenoemde nieuwe internationale verhoudingen ook tot spanningen kunnen leiden, zoals het geval is bij de ontwikkelingen in het 5G-dossier en de rol van het Chinese Huawei hierin.

De onderzoeksvragen
In dit rapport onderzoeken we hoe Nederlandse kennisinstellingen zich op een maatschappelijk verantwoorde manier kunnen verhouden tot de huidige ontwikkelingen, en wat hierin de rol is van de Nederlandse overheid. De centrale onderzoeksvraag in deze studie luidt:

Wat is er nodig om Nederlandse universiteiten en publieke onderzoeksinstituten op een verantwoorde manier te laten bijdragen aan kennisontwikkeling voor de defensie en veiligheid van Nederland en Europa?

Om deze vraag te beantwoorden, verhelderen we de huidige context waar Nederlandse universiteiten en publieke onderzoeksinstituten zich mee geconfronteerd zien. Dit doen we in vier hoofdstukken.

In het eerste hoofdstuk schetsen we de recente ontwikkelingen, met als centrale vraag: **hoe zien de nieuwe kennis- en innovatieagenda's voor defensie en veiligheid er wereldwijd uit?** Bij het beantwoorden van deze vraag laten we zien hoe de digitalisering van de samenleving in combinatie met veranderende internationale verhoudingen leidt tot een nieuwe digitale wapenwedloop, en

schenken we specifiek aandacht aan de nieuw kennis- en innovatieagenda's van de Verenigde Staten, China, Rusland, de Europese Unie en Nederland.

In het tweede hoofdstuk zetten we de huidige ontwikkelingen in een historisch perspectief: **wat zijn de verschillen tussen de historische en huidige kennis- en innovatieagenda's voor defensie en veiligheid?**

Hoofdstuk drie is een casestudy van het maritieme domein: **wat zijn de nieuwe kennis- en innovatieagenda's in het maritieme domein, en hoe verhouden die zich tot de agenda's uit het recente verleden?** Deze casus is gekozen omdat Nederland traditioneel gezien een sterke maritieme kennisbasis kent, en vormt een illustratie van de manier waarop de nieuwe kennis- en innovatieagenda's voor defensie en veiligheid ook doorwerken in dit traditionele militaire domein.

In hoofdstuk vier schetsen we een beeld van de uitdagingen die er momenteel liggen voor de Nederlandse universiteiten en publieke onderzoeksinstituten: **wat zijn de nieuwe uitdagingen voor de Nederlandse universiteiten en publieke onderzoeksinstituten?**

Op basis van de verheldering van de huidige context waarmee de Nederlandse universiteiten en publieke onderzoeksinstituten zich geconfronteerd zien, beantwoorden we in hoofdstuk vijf de hoofdvraag. Hiermee agenderen we de belangrijkste opgaven en dilemma's voor de komende jaren, en identificeren we op welk niveau - van individuele onderzoeker tot internationale verbanden - deze het beste kunnen worden geadresseerd.

Methode

Allereerst bestudeerden we wat de belangrijkste ontwikkelingen zijn op het gebied van kennisontwikkeling voor defensie en veiligheid, en hoe dit raakt aan het terrein van de Nederlandse universiteiten en publieke onderzoeksinstituten. De historische context is gebaseerd op deskresearch. Om de huidige ontwikkelingen beter te kunnen duiden, voerden we aan het begin van dit onderzoek, naast deskresearch, ook oriënterende gesprekken met een aantal experts uit het veld: Auke Venema en kolonel J.C. Dicke van het Ministerie van Defensie, Frank Bekkers van The Hague Centre for Strategic Studies (HCSS) en Margriet Drent en Dick Zandee van Clingendael. We willen hen daarvoor hartelijk danken.

Voor de casestudy hebben we gekozen voor het maritieme domein vanwege het feit dat Nederland van oudsher een sterke maritieme defensiesector kent. Momenteel is dit het enige domein waarin Nederland beschikt over een goede kennisbasis en een sterke industrie. Ook is Defensie van plan een groot deel van de Nederlandse vloot binnenkort te vernieuwen. De komende jaren staan in het

teken van de vervanging van onder meer onderzeeboten, fregatten en mijnenjagers. Dit brengt allerlei keuzes en dilemma's aan het licht die illustratief zijn voor de huidige dynamiek van kennis en innovatie voor defensie en veiligheid.

Ook voor de casestudy voerden we deskresearch uit en hielden we interviews met een aantal experts uit de sector. Om een zo compleet mogelijk beeld te krijgen, spraken we met deskundigen vanuit de overheid (ministerie van Defensie), het bedrijfsleven (Damen Shipyards en Thales Nederland), brancheorganisaties (Nederland Maritiem Land), universiteiten (TU Delft) en publieke kennisinstellingen (TNO en MARIN). Een lijst van geïnterviewden is als bijlage opgenomen.

1 Nieuwe kennis- en innovatieagenda's voor defensie en veiligheid

1.1 Veranderende internationale verhoudingen

In de publicatie 'Veiligheid in een wereld van verbindingen' stelt de WRR dat de veiligheidssituatie in en om Nederland is verslechterd. Deels wijst de WRR naar hoe burgeroorlogen in het Nabije Oosten en Afrika van invloed zijn op de Nederlandse situatie, bijvoorbeeld door terroristische dreigingen en de komst van vluchtelingen. Een andere concrete dreiging vormt de ontwrichtende invloed van Rusland, waarbij het gewapende conflict in Oekraïne een waarschuwingssignaal vormt. Ook ziet Nederland zich geconfronteerd met een breed spectrum aan nieuwe dreigingen, zoals hacken en desinformatie in het cyberdomein (WRR, 2017).

Op de achtergrond speelt dat geopolitieke verhoudingen zich in een fase van grondige herschikking bevinden: nieuwe mogendheden komen op en de voorheen als oppermachtig beschouwde Amerikaanse hegemonie wordt bedreigd. Met de opkomst van met name China vindt een verschuiving plaats van zowel economische als politieke macht. De WRR wijst ook op de toenemende economische en politieke invloed van landen als Rusland, Indonesië, India, Brazilië en Mexico. Er is geen sprake meer van een 'single global superpower', maar er ontstaat een nieuwe polycentrische wereldorde waarin diverse grootmachten naast elkaar bestaan (Arbatov, 2014).

Dit zal zich volgens de WRR vertalen in meer handelspolitieke spanningen, rivaliteit over de toegang tot grondstoffen en transportroutes, en uitbreiding van het militaire machtspotentieel. Daardoor ontstaan nieuwe uitdagingen op het gebied van *flow security*: de druk op de veiligheid van aanvoerroutes en het strategische spel om logistiek en verbindingen zal toenemen. Deze nieuwe geopolitieke verhoudingen creëren spanningen waar ook Nederland direct bij betrokken is. De tijd waarin Europa probleemloos kon schuilen onder een Amerikaanse veiligheidsparaplu is voorbij. De zorg voor de Nederlandse veiligheid belandt na een halve eeuw weer terug in eigen schoot.

1.2 Digitalisering als *gamechanger*

In de nieuwe geopolitieke werkelijkheid staan kennis en innovatie als strategisch middel voor economische en militaire macht weer bovenaan de politieke agenda. Dit is niet uniek. Ook in het verleden werden technologische superioriteit en voorsprong in kennis als cruciaal gezien om de tegenstander voor te blijven. Zo veroorzaakte buskruit een revolutie in de middeleeuwse oorlogvoering in Europa, en stond de Eerste Wereldoorlog in het teken van diverse technologische innovaties – van tanks en vliegdekschepen tot vlammenwerpers en gifgas. Berucht is ook de wapenwedloop tijdens en na de Tweede Wereldoorlog. Deze richtte zich in eerste instantie vooral op kennis over nucleaire fysica en het ontwikkelen van een kernwapenarsenaal, maar breidde snel uit. Verschillende overheden investeerden in onderzoekscentra en laboratoria voor defensieonderzoek en de ontwikkeling van een eigen defensie-industrie (Cops, 2018). Vaak wordt gewezen naar de VS en de Sovjet-Unie, maar ook de twee Europese 'winnaars' van de Tweede Wereldoorlog, het Verenigd Koninkrijk en Frankrijk, investeerden flink in militaire R&D en bouwden in deze tijd een relatief grote nationale industrie rondom defensie en veiligheid (Paillard & Butler, 2016).

Ook vandaag de dag leiden nieuwe technologische ontwikkelingen tot tal van nieuwe kansen en risico's op het gebied van defensie en veiligheid. Zo blazen biotechnologische ontwikkelingen de dreiging van biowapens nieuw leven in. In een tijdperk waarin klonen en 'designergenen' onderwerp zijn van het avondnieuws, is het ook mogelijk om micro-organismen genetisch te manipuleren voor doeleinden van biologische oorlogsvoering (Charlet, 2018).

Op het gebied van conventionele wapens is er vooral aandacht voor een nieuwe generatie hypersone raketten, die vijfmaal sneller dan het geluid op hun doel afgaan. Door hun hoge snelheid zijn hypersone raketten nauwelijks te onderscheppen. Deze wapens zijn niet per se bedoeld voor op het slagveld, maar kunnen worden gebruikt om strategische doelen als communicatiecentra of vliegdekschepen uit te schakelen. Het is wel mogelijk om er een bomlading op te bevestigen, conventioneel of nucleair. Zeker is dat alle grote landen, zoals China, India, Rusland en de VS, hypersone raketten ontwikkelen. Er wordt dan ook gevreesd dat de tijd van ontwapening voorbij is. Exemplarisch is het aflopen van het INF raketverdrag eind 2019. Zowel Rusland als de VS lijken niet in te zetten op een voortzetting van dat verdrag (Heirbaut, 2018).

De laatste jaren wordt met name de digitalisering van de samenleving gezien als de belangrijkste technologische ontwikkeling op het gebied van defensie en veiligheid. Daarom richten we ons in dit rapport specifiek op dat aspect.

We onderscheiden twee gebieden waarop digitalisering richtinggevend is voor defensie en veiligheid: nieuwe militaire innovaties en cyber als nieuw domein voor conflict. Hieronder bespreken we ze kort.

Digitalisering brengt nieuwe militaire innovaties

Nieuwe technologieën rondom kunstmatige intelligentie, automatisering en robotica kennen allemaal ook militaire toepassingen. *Virtual reality* leidt tot betere trainingsmogelijkheden voor militairen, en *augmented reality* moet soldaten ook in echte operaties ondersteunen met betere informatie. Hoogwaardige software moet in combinatie met big data helpen om beter geïnformeerde en snellere beslissingen te nemen (Spiegeleire & Sweijs, 2017). Veel aandacht gaat naar mens-machine interactie. Naarmate machines slimmer en hierdoor ook autonomer worden, ontstaat een andere taakverdeling tussen mens en machine. Deze mens-machine interactie moet leiden tot een effectievere en efficiëntere samenwerking, waarbij machines bepaalde fysieke en cognitieve taken ondersteunen of overnemen (Ministerie van Defensie, 2016). Veel ontwikkelingen op het gebied van volledig autonome systemen zitten nu nog in de pilotfase, maar het lijkt waarschijnlijk dat de forse R&D-inspanningen de komende tijd tot een explosie van daadwerkelijke toepassingen zullen leiden. In toekomstvisies wordt bijvoorbeeld al gesproken over *killer robots* die soldaten achterhaald moeten maken en autonome ‘zwermen’ van drones die conventionele legers machteloos laten (Geveke, 2017).

Cyber als nieuw domein voor conflict

Met de opkomst van de digitale samenleving wordt ‘cyber’ naast land, zee, lucht en ruimte, vaak gezien als het vijfde domein van conflict (Ministerie van Defensie, 2016). Het cyberdomein kent een breed palet aan instrumenten van dreiging en conflict, zoals cyberspionage waarmee staats- of bedrijfsgeheimen kunnen worden ontfutseld, desinformatie waardoor samenlevingen kunnen destabiliseren, en cyberwapens die vitale infrastructuur kunnen saboteren en mogelijk grote schade kunnen aanrichten (Munnichs et al, 2017). In de afgelopen jaren heeft een aantal incidenten nieuwe vormen van cyberconflict aan het licht gebracht. Bekende voorbeelden zijn de vermeende sabotage van Iraanse kerncentrifuges door de Amerikanen, beïnvloeding van de Amerikaanse presidentsverkiezingen met behulp van nepnieuws door de Russen, en diverse beschuldigingen van bedrijfsspionage door de Chinezen (Hamer & van Est, 2019).

Met cyber als nieuw domein voor conflict, brengt de digitale samenleving ook tal van nieuwe kwetsbaarheden met zich mee. Cyberaanvallen richten zich regelmatig op de civiele infrastructuur, waarbij juist de burger wordt geraakt. Denk aan nieuwe kwetsbaarheden bij de waterinfrastructuur, de banken, energiebedrijven en zorginstellingen.

Vanuit dit perspectief is de opkomst van ‘the internet of things’ en de aanstaande uitrol van een 5G-netwerk niet alleen een civiele aangelegenheid, maar een ontwikkeling die ook vanuit defensie- en veiligheidsoogpunt grote gevolgen heeft.

1.3 Nieuwe kennis- en innovatieagenda’s voor defensie en veiligheid

Digitalisering brengt tal van nieuwe kennis- en innovatiebehoeften voor defensie en veiligheid: de behoefte om voorop te lopen in nieuwe strategische technologieën, om te beschermen tegen nieuwe kwetsbaarheden, en aan capaciteitsopbouw voor conflicten in het cyberdomein. Wereldwijd komen landen in beweging en ontvouwt zich een technologische race rondom digitale sleuteltechnologieën.

In de praktijk betekent dit dat militaire grootmachten zoals de Verenigde Staten, China en Rusland nieuwe kennis- en innovatieagenda’s formuleren. Ook de EU, die zich lang uitsluitend op civiele zaken richtte, begint zich te manifesteren als een speler van belang.

In deze paragraaf beschrijven we eerst de ontwikkelingen in de Verenigde Staten, China, Rusland en de EU. Vervolgens beschrijven we de belangrijkste ontwikkelingen in Nederland.

1.3.1 Verenigde Staten

In 2014 gaf de VS een nieuwe impuls aan haar kennis- en innovatieagenda’s voor defensie onder de naam *third offset strategy*, waarin *offset* doelt op het voorsprong gevende effect van technologische superioriteit (Louth & Moelling, 2016). Al decennia lang besteedt de VS meer aan militaire R&D dan welk ander land ter wereld. Technologische superioriteit wordt als cruciaal gezien om de tegenstander voor te blijven. De eerste o*ffset strategy* stamt uit 1952 en had als doel een voorsprong te ontwikkelen ten opzichte van de Russen op het gebied van kernwapens. De tweede *offset strategy* stamt uit de jaren ‘80 en had als doel een voordeel in de confrontatie te creëren door een samenspel van *intelligence*, precisienavigatie en niet-waarneembare *stealth*-voertuigen. Dit maakte *seeing deep, shooting deep* mogelijk, wat de mogelijkheid gaf tot gerichtere interventies van grotere afstand, met minder risico voor eigen personeel en materieel. De VS demonstreerde het succes van deze strategie in de Eerste Golfoorlog van begin jaren ‘90, waar de tegenstander in voornamelijk Russische pantservoertuigen een gemakkelijk doelwit vormde (Martinage, 2014).

De nieuwe, derde, *offset strategy* is een poging om teruglopende technologische superioriteit te voorkomen, ten opzichte van met name het opkomende China. Nadruk ligt op digitale technologieën zoals robotica, autonome wapensystemen, mens-machine integratie, big data analyse en cybercapaciteiten voor zowel offensieve als defensie doeleinden (Martinage, 2014; Louth & Moelling, 2016). Zo spendeert het Amerikaanse ministerie van Defensie jaarlijks 7,4 miljard dollar aan 'geclassificeerd' (geheim) onderzoek naar kunstmatige intelligentie (Polyakova, 2018). De totale investering in deze nieuwe strategie is moeilijk te achterhalen. Deels bestaat de strategie uit nieuwe onderzoeksprogramma's. Zo werd in 2017 201 miljoen dollar vrijgemaakt in mens-machine *teaming*, en 309 miljoen dollar voor cyberoorlogsvoering. Deels bestaat het programma uit de opschaling van bestaande programma's, met een belangrijke verschuiving in de interne financieringsprioriteiten. Zo komt er binnen de marine bijvoorbeeld meer nadruk te liggen op autonome zeedrones voor onderwateroorlog (Eaglan, 2016).

Onder president Trump spreekt de regering overigens niet meer openlijk over een *third offset strategy*, maar dat wil niet zeggen dat deze strategie niet meer bestaat. Bovenstaande voorbeelden zijn slechts enkele voorbeelden van tal van programma's die de nadruk leggen op doorbraken in nieuwe digitale sleuteltechnologieën. Met als doel de Amerikaanse militaire technologische superioriteit te herstellen.

1.3.2 China

In 2015 lanceerde de Chinese overheid de beleidsplannen *Made in China 2025* Hierin spreekt China de ambitie uit om zelfvoorzienend te worden op het gebied van kennis en innovatie in tal van strategische sectoren, en koploper te worden op het gebied van opkomende strategische technologieën zoals kunstmatige intelligentie en robotica (Kennedy, 2015). Deze strategie richt zich zowel op civiele als op militaire toepassingen. Lange tijd had het Chinese leger een grote technologische achterstand op Rusland en de Verenigde Staten. Maar met de snelle industrialisering van China in de afgelopen dertig jaar, is ook het leger gaan moderniseren.

Tot 2030 zal de Chinese overheid 150 miljard dollar investeren in het ontwikkelen van een industrie rondom de strategische technologieën (Polyakova, 2018). Zo wordt twee miljard dollar geïnvesteerd in het opzetten van een *AI research campus* waar zich 400 bedrijven moeten gaan vestigen (Kharpal, 2018). Een voorbeeld van een militaire toepassing die nu door China wordt ontwikkeld, is een *drone swarm*: een grote vloot drones die via geavanceerde software in staat zijn tot zelforganisatie en coördinatie.

Drones kunnen worden uitgerust met allerhande wapens, waardoor massale, strak uitgevoerde aanvallen mogelijk worden. Conventionele voertuigen en wapensystemen zijn niet ingericht om zich te verweren tegen zwermen, wat de *drone swarms* een grote bedreiging maakt. China voerde in 2017 een testmissie uit met een vloot van 119 drones, de grootste tot nu toe (Feng & Clover, 2017).

Dankzij Chinese inspanningen is de toekomstige koppositie van de VS op technologisch gebied niet vanzelfsprekend. Men spreekt ook wel van een race om *AI supremacy*, een technologische race die zich met name tussen de VS en China afspeelt (The Economist, 2018). Op een aantal technologische gebieden is China al een wereldmacht, bijvoorbeeld in het cyberdomein. Dit werd voor het eerst merkbaar rond 2008, toen China economische spionageaanvallen op Amerikaanse en Europese bedrijven uitvoerde (Inkster, 2017). De aanvallen gingen onder meer om diefstal van intellectueel eigendom. Op dit moment geldt dat China slechts op bepaalde technologieën al zelfvoorzienend is; voor andere technologieën, zoals halfgeleiders, is het land nog afhankelijk van westerse bedrijven.

Net als met de *third offset strategy* van de Amerikanen, noemt de Chinese overheid de strategie niet meer expliciet *Made in China 2025*. Waarschijnlijk omdat andere landen het onder die noemer te veel als bedreiging zagen. Wel zijn de achterliggende beleidsplannen nog steeds een feit.

1.3.3 Rusland

Ook in Rusland is vanaf 2010 een moderniseringsslag ingezet. Hierbij is veel geïnvesteerd in kunstmatige intelligentie, met als doel dat tegen 2025 het militaire materieel voor 30 procent uit autonome gerobotiseerde systemen bestaat (The Economist, 2014). Hoewel Rusland met ongeveer vier procent een groot percentage van het bruto binnenlands product aan defensie besteedt, is het budget nog geen tiende van dat van de VS, en ongeveer een derde van dat van China (Bitzinger & Popescu, 2017). In hoeverre Rusland mee kan in de technologische race tussen die twee grootmachten, is dan ook de vraag. Precieze uitgaven zijn niet bekend, maar verschillende rapporten schatten dat de uitgaven aan onderzoek naar kunstmatige intelligentie ongeveer 12,5 miljoen dollar per jaar zijn - een fractie van wat grootmachten China en de VS jaarlijks uitgeven (Polyakova, 2018).

In 2014 werd de Russische moderniseringsslag dan ook verankerd in een nieuwe doctrine, waarin hybride oorlogsvoering en verbreding van het militaire instrumentarium centraal staan (Chivvis, 2017). Het achterliggende idee is dat het land de voorsprong van de VS wat betreft hightech-wapens niet gemakkelijk kan inhalen. Met nieuwe technologische paden en inzet op *grey area conflict* hoopt

Rusland meer geopolitiek effect te sorteren (Polyakova, 2018). Zo zet het sterk in op offensieve capaciteiten in het nieuwe cyberdomein. Ook zijn er legio voorbeelden van Russische pogingen tot hacken en cyber-fysieke aanvallen, zoals het stilleggen van energiecentrales in Oekraïne. Daarnaast zet Rusland in op beïnvloeding en destabilisering van het publiek debat en instituties in andere landen, met als toppunt de inmenging in de Amerikaanse presidentsverkiezingen van 2016 (Hamer et al., 2019).

1.3.4 De Europese Unie

Ook de Europese Unie kondigde significante investeringen aan in onderzoek voor defensie en veiligheid. Voor de volgende begrotingsronde, die loopt van 2021 tot 2027, heeft de Europese Commissie een Europees Defensiefonds voorgesteld ter waarde van 13 miljard euro. Hiermee zou het budget van de EU in omvang het vierde budget van Europa zijn, na Frankrijk, de VK en Italië. Het fonds is bedoeld voor de bevordering van een innovatieve en concurrerende industriële defensiebasis en moet bijdragen aan de strategische autonomie van de EU. In februari 2019 is dit voorstel aangenomen, onder voorbehoud van formele goedkeuring door het Europees Parlement en de Raad. Voor financiering van Europese projecten voor defensieonderzoek is 4,1 miljard euro gereserveerd. Voor het geval dat er minimaal drie Europese landen beslissen om samen industriële defensiecapaciteiten op te bouwen, is er 8,9 miljard euro gereserveerd voor het aanvullen van nationale bijdragen (Europese Commissie, 2019).

Deze Europese aandacht is nieuw. Met de Tweede Wereldoorlog nog vers in het geheugen moest de EU nadrukkelijk een civiel project worden. Samenwerking op het gebied van defensie en veiligheid was expliciet uitgesloten. De Europese rol op defensiegebied kreeg met name vorm door de inspanningen van de twee Europese ‘winnaars’ van de Tweede Wereldoorlog: het VK en Frankrijk. Beide landen bouwden een relatief grote nationale industrie rondom defensie. Hoewel Europese integratie in de jaren ’80 en ’90 van de vorige eeuw verder groeide en meer beleidsterreinen ging omvatten, bleven veiligheid en defensie uitgesloten van de gezamenlijke Europese beleidsagenda. Europa moest een civiel project blijven (Karempekios et al., 2018).

In het begin van de 21ste eeuw ontstond er een voorzichtige kentering, die ook te zien is in het Europese onderzoeks- en innovatiebeleid. Zo introduceerde het zesde

Europese kaderprogramma[1] (FP6, dat liep van 2002 tot 2006) de *Preparatory Action on Security Research* (PASR). Hiermee begon de overgang van exclusief civiel naar defensie-gerelateerd EU-onderzoek. In het zevende kaderprogramma (FP7, dat liep van 2007-2013) volgde de volwaardige introductie van het thema veiligheid onder de zogeheten *European Security Research Programme* (ESRP), met een focus op het ontwikkelen van veiligheidstechnologieën. In Horizon 2020, het kaderprogramma voor 2014 tot 2020, is 'een veilig Europa' zelfs benoemd tot één van de zeven maatschappelijke uitdagingen (Karempekios et al., 2018).

Sinds 2013 is de Europese Commissie zich langzamerhand ook gaan richten op defensie. Zo publiceerde de Europese Commissie in 2014 een White Paper over de noodzaak van gezamenlijk Europees defensieonderzoek. Onder Horizon 2020 volgde een *Prepatory Action on Defense Research* (PADR). Voor het eerst in de Europese geschiedenis stimuleert de EU Europese defensiesamenwerking, met een budget van 590 miljoen euro. Daarvan is 90 miljoen euro bedoeld voor onderzoek en 500 miljoen euro voor de ontwikkeling van gezamenlijke industriële capaciteiten (Europese Commissie, 2019)

De civiele nalatenschap van het Europese project blijft deels bestaan. Waarschijnlijk komt er geen onderzoeksgeld voor klassieke wapenindustrie. Prioriteit wordt gegeven aan sleuteltechnologieën zoals kunstmatige intelligentie, robotica en augmented reality. Zo is er 100 miljoen uitgetrokken om de ontwikkeling van een Europese drone te ondersteunen (de Eurodrone). Ook is er veel aandacht voor categorieën die worden aangeduid als opkomende *gamechangers*, zoals autonome navigatie, kunstmatige intelligentie, kwantumtechnologieën en technologieën om de fysieke en mentale vermogens van soldaten te vergroten (Wallace, 2019).

1.3.5 Nederland

Ook in Nederland krijgt kennisontwikkeling voor defensie en veiligheid een nieuwe impuls vanuit de overheid. Met het Regeerakkoord van eind 2017 en de daaropvolgende defensienota van begin 2018 breekt Nederland met een trend. Na jaren van bezuiniging kantelt het politieke klimaat rondom defensie en veiligheid. Het zogeheten 'vredesdividend' van de jaren '90 lijkt uitgeput, en een hernieuwd gevoel van urgentie leidt tot nieuwe investeringen. Die financiële impuls moet leiden tot een verdubbeling van het defensiebudget over tien jaar tijd.

---

[1] De Europese Commissie stuurt haar onderzoeks- en innovatiebeleid aan door middel van zogeheten kaderprogramma's. Het eerste kaderprogramma werd goedgekeurd in 1983. Momenteel loopt het achtste kaderprogramma, beter bekend als Horizon 2020. Het negende kaderprogramma, Horizon Europe, zal in 2020 van start gaan.

Een groot deel zal worden gebruikt voor ‘achterstallig onderhoud’ van het materieel en investeringen in het welzijn van het defensiepersoneel, maar ook de R&D-uitgaven zullen stijgen. Naast initiatieven vanuit het ministerie van Defensie, begeven ook andere miniseries zich nadrukkelijker op het terrein van kennisontwikkeling voor defensie en veiligheid. Hieronder bespreken we een aantal in het oog springende initiatieven.

Ministerie van Defensie
In de loop van 2018 verschijnen er drie publicaties die meer inhoud geven aan de nieuwe koers die Nederland uitzet voor defensie, te weten de Defensie Industrie Strategie, de Defensie Cyberstrategie en de Innovatiestrategie Defensie. We lichten ze hieronder kort toe. Met die strategieën wordt bepaald welke kennis en capaciteiten noodzakelijk zijn om de belangen van nationale veiligheid te beschermen en wat er nodig is om die kennisbasis te borgen.

A. Defensie Industrie Strategie
De Defensie Industrie Strategie (DIS) schetst een wereld in verandering en benadrukt dat Nederland zich moet kunnen blijven beschermen tegen alle bestaande en nieuwe dreigingen. De doelstelling van de DIS is weergeven welke kennis en capaciteiten van het bedrijfsleven en kennisinstellingen nodig zijn om de nationale veiligheidsbelangen te beschermen en hoe die kennisbasis geborgd kan worden. Het belang van internationale samenwerking wordt erkend, maar de DIS stelt ook dat Nederland zelfstandig moet kunnen beschikken over kennis en capaciteiten voor het dienen van de nationale veiligheidsbelangen. Nederland moet een geloofwaardige partner zijn in internationale samenwerkingsverbanden. Hiermee breekt de nieuwe DIS met de vorige strategie uit 2013, waaruit de nadrukkelijke voorkeur bleek voor het elders kopen van spullen. De DIS uit 2018 pleit voor een minder naïef beleid, om daarmee de belangen van de Nederlandse industriële basis beter te beschermen. Zo stelt de DIS dat Defensie bij toekomstige aanbestedingsprocedures waar mogelijk – en binnen de kaders van de Europese regelgeving – zal kiezen voor Nederlandse leveranciers. Als dit niet direct mogelijk is, wil Defensie er in ieder geval voor zorgen dat Nederlandse bedrijven en kennisinstellingen worden betrokken bij de productie. Om de Nederlandse veiligheidsbelangen te beschermen, gaat Defensie ook kritisch kijken naar buitenlandse overnames in de Nederlandse defensie- en veiligheidsindustrie.

B. Defensie Cyber Strategie
De Defensie Cyber Strategie (CBS) stelt dat kennisontwikkeling en innovatie op het gebied van cybersecurity nodig is om tegenstanders voor te blijven en nieuwe digitale dreigingen het hoofd te kunnen bieden. Bovendien stelt de strategie dat een hoogwaardige, autonome kennispositie kan zorgen dat Defensie minder afhankelijk wordt van cybersecurity-expertise en -oplossingen van anderen.

Defensie werd in 2018 lid van het NWO-programma Dcypher om hiermee een actieve bijdrage te kunnen leveren aan de agendering en coördinatie van cybersecurityonderzoek in Nederland. Ook droeg Defensie actief bij aan de totstandkoming van de Nationale Cybersecurity Research Agenda.
Eigen investeringen in cyberonderzoek nemen toe: van 4 miljoen euro in de voorbije jaren tot 6,5 miljoen per jaar in 2019. Defensie spreekt de intentie uit om dit waar mogelijk samen met andere departementen te doen.

C. Innovatiestrategie Defensie

Het uitgangspunt van de nieuwe Innovatiestrategie van Defensie is dat het ministerie tijdig moet kunnen inspelen op de kansen en mogelijkheden voor het verbeteren van zijn operationele effect, voortkomend uit ontwikkelingen in de samenleving, technologie en wetenschap. De innovatiestrategie specificeert hoe Defensie innovaties beter en sneller kan absorberen. Het gaat daarbij expliciet niet alleen om technologische innovaties, maar ook om tal van sociale en organisatorische innovaties en daarmee gepaard gaande culturele veranderingen. De focus ligt sterk op de rol van mensen, het creëren van ruimte voor experiment, het stimuleren van de juiste *mindset* en nieuwe manieren van denken, en op samenwerking in multidisciplinaire teams van partijen binnen en buiten defensie.

Ministerie van Justitie & Veiligheid

Naast het ministerie van Defensie zien we dat ook andere partijen kennis- en innovatieagenda's aanwenden voor defensie- en veiligheidsdoeleinden, zoals het ministerie van Justitie en Veiligheid (J&V). Van oudsher is de kennisbasis van J&V vooral ingericht voor het verkrijgen van kennis over beleid, bijvoorbeeld door beleidsrelevant onderzoek uit te zetten bij het Wetenschappelijk Onderzoek- en Documentatie Centrum. De laatste jaren ziet het ministerie van J&V ook het belang van (technologische) kennis en innovatie voor de veiligheid van Nederland. Zo is in 2017 voor het eerst een eigen strategische kennis- en innovatieagenda (SKIA) ontwikkeld, die de bredere kennis- en innovatiebehoeften van het ministerie in kaart brengt. Het meest in het oog springende initiatief is het meerjarige programma *Innoveer mee met J&V*, waarin de samenleving wordt uitgedaagd om met innovatieve oplossingen te komen voor het verbeteren van de veiligheid van Nederland. Dit programma bestaat uit diverse symposia en congressen, en is gekoppeld aan verschillende initiatieven, zoals innovatieve pre-competitieve aanbestedingen, een *startup-in-residence* programma en een Veiligheid Innovatie Competitie voor studenten.

Ministerie van Buitenlandse Zaken

Het ministerie van Buitenlandse Zaken is van oudsher een belangrijke partij in het vormgeven van een kennisbasis over strategisch en beleidsondersteunend onderzoek op het gebied van internationale (veiligheids)politiek.

In 2016 bundelden het ministerie van Defensie en Buitenlandse Zaken deze behoefte met elkaar. Tot voor kort bestond er een directe subsidierelatie met Clingendael, maar deze is inmiddels afgebouwd en vervangen door een contractuele relatie, waarbij ook regelmatig een beroep wordt gedaan op de expertise van onderzoekers van het HCSS, het The Hague Centre for Strategic Studies.

Ministerie van Economische Zaken en Klimaat

Ook bij het ministerie van Economische Zaken en Klimaat staan kennis en innovatie voor defensie en veiligheid op de agenda. *Veiligheid* is benoemd tot één van de vier maatschappelijke uitdagingen die richting moeten geven aan het Nederlandse innovatiebeleid; onder andere door veiligheid onderdeel te maken van het topsectorenbeleid. Een concrete uiting hiervan is de roadmap 'security', opgesteld in 2018 door de topsector High-Tech Systemen en Materialen (HTSM). Deze roadmap moet de komende decennia leiden tot innovaties die de nationale veiligheidsbelangen van Nederland kunnen beschermen. Om dit te verwezenlijken is samenwerking nodig tussen de hightech-industrie en de nationale defensie- en veiligheidsindustrie.

In april 2019 heeft het kabinet ook 25 missies vastgesteld voor het topsectoren- en innovatiebeleid. Onder het thema Veiligheid zijn onder leiding van het ministerie van Defensie en het ministerie van Justitie & Veiligheid zes missies[2] geformuleerd die moeten bijdragen aan een veiliger samenleving, een weerbaarder Nederland, én het creëren van economische kansen. De missies hebben een brede insteek. Uitgangspunt is dat in het veiligheidsdomein niet alleen nieuwe technische kennis moet worden ontwikkeld, maar dat er ook behoefte is aan sociaal, maatschappelijk, juridisch, gedragswetenschappelijk, organisatorisch, sociaalpsychologisch en (geo)politiek onderzoek. Nadruk ligt op samenwerken tussen overheid (genoemd worden de ministeries van BZK, J&V, DEF, EZK en OCW), bedrijfsleven (specifiek wordt verwezen naar Topsectoren HTSM, ICT, Logistiek, Creatieve Industrie, Water en Maritiem) en kennisinstellingen (genoemd worden NWO, TNO, NLR, Marin, universiteiten en hogescholen).

Ministerie van Onderwijs, Cultuur en Wetenschap

Tenslotte ontwikkelt ook het ministerie van OCW nieuwe kennis- en innovatieagenda's, met name op het gebied van cybersecurity. Zo heeft NWO in 2011 voor het eerst een Nationale Cybersecurity Research Agenda opgesteld. In 2018 is de derde editie hiervan gepubliceerd. Ook is Cybersecurity een speerpunt van NWO-EW (exacte wetenschappen).

---

2 De zes missies zijn: Integrale aanpak van georganiseerde criminaliteit; Maritieme hightech voor een veilige zee; Veiligheid in en vanuit de ruimte; Cyberveiligheid; Genetwerkt optreden op land en vanuit de lucht; en Samen sneller innoveren voor een adaptieve krijgsmacht.

Daarnaast is vanuit NWO ook het eerdergenoemde platform Dcypher opgericht, met als doel agendering en coördinatie van zowel wetenschappelijk als praktijkgericht cybersecurity-onderzoek.

1.4 Conclusie

In dit hoofdstuk brachten we in kaart hoe de nieuwe kennis- en innovatieagenda's voor defensie en veiligheid in verschillende landen eruitzien. Drijvende krachten achter de nieuwe agenda's zijn een verslechterde veiligheidssituatie en nieuwe internationale spanningen. Hierdoor staan kennis en innovatie, als strategisch middel voor economische en militaire macht, hoog op de agenda.

Digitalisering wordt gezien als een belangrijk strategisch kennisveld voor defensie- en veiligheidsvraagstukken, waarmee zich een technologische wedloop ontvouwt rondom een aantal digitale sleuteltechnologieën. De VS en China spelen hierin een belangrijke rol. Rusland is financieel minder krachtig, maar door een slimme doctrine en strategische inzet van nieuwe technologie is het een belangrijke partij in dit nieuwe krachtenveld. Ook de EU, die zich van oorsprong een uitsluitend civiele taak toedichtte, begint zich steeds meer te manifesteren op dit gebied. In het nieuwe begrotingsfonds, dat zal lopen van 2021 tot 2027, zal naar alle waarschijnlijkheid 13 miljard euro worden uitgetrokken voor een Europees Defensiefonds.

In Nederland geven het regeerakkoord uit 2017 en de defensienota uit 2018 een flinke impuls aan defensie-uitgaven, ook voor kennis en innovatie. Daarbij is veel aandacht voor digitalisering en de opkomst van cyber als nieuw domein voor conflict. Ook andere ministeries formuleren steeds nadrukkelijker kennis- en innovatieagenda's voor defensie en veiligheid.

2 Kennisontwikkeling voor defensie en veiligheid in de digitale samenleving

Kennis en innovatie als strategisch middel voor zowel economische als militaire macht staan weer bovenaan de politieke agenda. Het vorige hoofdstuk schetste een beeld van hoe kennisecosystemen wereldwijd worden gemobiliseerd voor defensie- en veiligheidsdoeleinden.

Ook in het verleden werden technologische superioriteit en voorsprong in kennis als cruciaal gezien om de tegenstander voor te blijven. In dit hoofdstuk schetsen we eerst de belangrijkste eigenschappen van deze militaire kennisecosystemen uit het verleden, met aandacht voor de specifieke kenmerken van de Nederlandse context.

Vervolgens laten we zien dat de huidige situatie verschilt van deze historische context. In vergelijking met de wapenwedloop tijdens de Koude Oorlog, kent de huidige technologische race een andere dynamiek, gekenmerkt door een grensvervaging tussen militair en civiel, en een grote internationale verwevenheid.

2.1 Het ontstaan van nationale militaire kennisecosystemen

In de periode tijdens en na de Tweede Wereldoorlog kreeg ontwikkeling van nieuwe technologieën met militaire toepassingen hoge prioriteit. De Koude Oorlog leidde tot een wapenwedloop tussen met name de VS en de Sovjet-Unie. Ook het Verenigd Koninkrijk en Frankrijk bouwden in deze tijd een relatief grote nationale industrie rondom defensie en veiligheid. In de jaren ‘60 verwees de toenmalige Amerikaanse president Eisenhower naar deze industrieën als het ‘militair-industrieel complex’.

Kennisontwikkeling was in die context van strategisch belang. Zo was er veel aandacht voor kennis over nucleaire fysica, cruciaal voor het ontwikkelen van een kernwapenarsenaal. Maar de focus was breder en heel wat overheden investeerden in verschillende onderzoekscentra en laboratoria voor defensie-onderzoek, met elk een eigen specialisme (Cops, 2018). Dergelijke investeringen resulteerden in het ontstaan van militaire kennisecosystemen, die veelal duidelijk te onderscheiden waren van civiele kennisecosystemen.

Gezien het belang van wetenschappelijke kennis worden deze kennisecosystemen ook wel aangeduid als ‘wetenschappelijk-militair-industrieel complex’ (Smart, 2016).

De militaire kennisecosystemen die werden gemobiliseerd voor dit wetenschappelijk-militair-industrieel complex, voldeden aan een aantal specifieke kenmerken:

- **Duidelijke grenzen tussen militaire en civiele kennisecosystemen**. De militaire kennisecosystemen werden gevormd door een duidelijk afgebakende kennisinfrastructuur van gespecialiseerde laboratoria en bedrijven. Ze onderscheidden zich door andere actoren, andere aanbestedingsbehoeften, andere kwaliteitsnormen en andere toeleveringsnetwerken. Binnen deze kennisecosystemen werd veel nieuwe, vaak ook fundamentele, kennis ontwikkeld (Mollas-Gallart, 2009). De meest bekende voorbeelden hiervan komen uit Amerika, zoals het Manhattan Engineering District (MED), dat tijdens WOII de atoombom ontwikkelde.

- **De militaire kennisecosystemen waren missiegedreven.** Militaire kennisecosystemen werden gemobiliseerd door duidelijke missies rondom een aantal strategische technologieën. Ministeries van defensie speelden als betrokken en intelligente ‘launching customers’ een centrale rol in agendering en financiering (Mowery, 2012). De verschillende laboratoria werden top-down aangestuurd door een centrale organisatie, zoals het in de Verenigde Staten in 1957 opgerichte *Defense Advanced Research Projects Agency* (DARPA). Dit leidde tot een separate markt voor militair onderzoek en innovatie, aangestuurd op basis van duidelijke specificaties, standaarden en regulering.

- **Het wetenschappelijk systeem was gesloten en kenmerkte zich door geheimhouding**. Militaire kennisecosystemen hadden een andere dynamiek van kennisproductie en circulatie dan de civiele kennisecosystemen. Ze werden gekenmerkt door geslotenheid en geheimhouding. Hierdoor ontstond een wetenschappelijke cultuur waarin wetenschappers de volledige vrijheid hadden om te werken aan (geheime) projecten, zonder de wetenschappelijke mores van externe *peer review* en publicatiedruk (James, 2009).

- **Het kennisecosysteem was nationaal georganiseerd.** De combinatie van geheimhouding en nationale veiligheidsbelangen zorgde voor een kennisecosysteem dat op nationale schaal functioneerde (Mowery, 2012).

- **Militaire kennisecosystemen waren sterk gelinkt aan nationale defensie-industrieën.** Wederom is Amerika hier het beste voorbeeld, maar ook in

Europa ontstonden tijdens de Koude Oorlog grote defensie-industrieën. Onder meer in landen als het Verenigd Koninkrijk, Frankrijk, Zweden, Italië en Spanje, en in mindere mate in Nederland (Mowery, 2012).

- **Militaire R&D kende een grote innovatiedynamiek.** Defensie was in de twintigste eeuw lange tijd een belangrijke motor achter technologische innovatie en liep voor op de civiele markt. De Koude Oorlog stimuleerde uitgaven in militaire R&D, met name in de VS, waar militaire R&D zelfs meer dan 50 procent van het totale R&D-budget ontving (James, 2009). Deze grote innovatiedynamiek uitte zich in het *spilloverfenomeen*: veel van de militaire R&D-projecten vonden uiteindelijk civiele toepassingen. Een bekend voorbeeld is de iPhone, die gezien kan worden als een samenvoeging van verschillende innovaties met hun oorsprong in het Amerikaanse militair-industriële complex (Mazzucato, 2013).

2.2 Militaire kennisecosystemen in Nederland

Ook Nederland gaf na de Tweede Wereldoorlog vorm aan nationale militaire kennisecosystemen. De omvang ervan was vanzelfsprekend niet te vergelijken met die van de VS, of dichter bij huis het VK of Frankrijk. Toch kende Nederland een serieuze militaire industriële basis op zowel land (DAF) en in de lucht (Fokker), als met name op zee (diverse scheepswerven zoals Damen, RSV en RH Marine). Ook had Nederland verschillende munitiefabrikanten zoals Eurometaal, Kruithoorn en Muiden Chemie. Philips was vanuit het NatLab in het eerste decennium na de oorlog zeer nauw betrokken bij het Nederlands defensieonderzoek, en leverde zowel fundamentele onderzoeksresultaten als technologische toepassingen.

Over de rol van deze bedrijven valt veel te zeggen. Wij richten ons in dit onderzoek echter op de rol van de publieke kennisinfrastructuur – bestaande uit universiteiten, wetenschappelijke instituten en publieke kennisorganisaties. Verschillende wetenschappelijke disciplines speelden een belangrijke rol in defensieonderzoek. Ten eerste de natuurkunde, met name op het gebied van atoom- en molecuulfysica, elektronica, en optica. Bekende toepassingen zijn radar- en sonarapparatuur, vuurgeleiding gebaseerd op radar of sonar (voor schieten met zwaar geschut), nabijheidsbuizen (voor het op het juiste moment tot ontploffing brengen van granaten of raketten) en diverse andere vormen van detectie, zoals infrarood-nachtkijkers. Daarnaast leverde het chemisch en medisch-biologisch onderzoek in Nederland vele toepassingen op militair gebied – zowel in offensieve als in defensieve zin. Tot slot zijn er diverse andere vakgebieden die een rol speelden in defensieonderzoek, maar vaak minder aandacht kregen – van wiskunde en logica tot bestuurskunde en psychologie (Hoeneveld, 2018).

In onderstaande paragrafen bespreken we kort de rol van TO2-instellingen (toegepast-onderzoek-organisaties), wetenschappelijke instituten en universiteiten.

2.2.1 Rol van publieke kennisorganisaties

Ook Nederland investeert na de Tweede Wereldoorlog in speciale onderzoekscentra en laboratoria voor defensieonderzoek. Dit onderzoek vindt hoofdzakelijk plaats binnen de muren van vijf publieke kennisorganisaties: TNO, NLR, MARIN, Clingendael en de Nederlandse Defensie Academie (NLDA). Publieke kennisorganisaties doen wetenschappelijk onderzoek, gericht op een bepaald onderwerp, en combineren dat met kennisintensieve dienstverlening. Hun bestaansrecht ligt bij deze kennisintensieve dienstverlening, en niet primair bij kennisvermeerdering door onderzoek, zoals bij universiteiten (Koens et al., 2017).

TNO heeft op het gebied van defensie en veiligheid een brede onderzoeksagenda, voornamelijk gericht op toegepast natuurwetenschappelijk onderzoek. MARIN en NLR hebben een specifiekere taak en hun defensie-gerelateerd onderzoek richt zich respectievelijk op de marine en de luchtmacht. Clingendael is een Nederlands kennisinstituut dat diverse aspecten van de internationale betrekkingen bestudeert. De NLDA is een militaire academie die ook zelfstandig onderzoek doet op het gebied van militaire wetenschappen en militaire historie.

Historisch gezien heeft TNO van alle publieke kennisorganisaties veruit de grootste rol. Deze rol krijgt in 1946 gestalte met de oprichting van de Rijksverdedigingsorganisatie van TNO (de RVO), een samenvoeging van drie kleinere laboratoria. De Rijksverdedigingsorganisatie van TNO wordt het ‘huislaboratorium’ van Defensie: de minister van Defensie en de krijgsmacht stellen de onderzoeksagenda vast; 90 procent van de financiering komt direct vanuit de overheid. Onderzoekers werken grotendeels achter gesloten deuren. De Rijksverdedigingsorganisatie maakt een spectaculaire groei door: van ongeveer 90 medewerkers in 1948 tot 790 in 1972. Daarna loopt het aantal geleidelijk op tot ongeveer 940 medewerkers in 1990, het hoogtepunt qua omvang (Lintsen, 2012).

Het grootste laboratorium van de RVO was het Physisch Laboratorium.
Het laboratorium speelde een centrale rol in het Nederlandse defensieonderzoek, vanwege het belang van de natuurkunde. Belangrijke onderzoeksprogramma’s van het laboratorium waren de ontwikkeling van radar- en sonartechniek, en mechanische en digitale vuurleiding gebaseerd op radar of sonar. Daarnaast onderzocht het laboratorium diverse infraroodtechnieken en de mogelijkheid van raketbouw. Ook was er een Technologisch Laboratorium waar explosieven en motoren werden getest (Lintsen, 2012).

Onderzoek gebeurde zowel op het gebied van defensie als van veiligheid. Voor veiligheid was er vooral een belangrijke rol voor het Chemisch laboratorium en het Medisch-Biologisch laboratorium, waar onderzoek werd gedaan naar de gevolgen van nucleaire, biologische en chemische oorlogvoering, en de mogelijke bescherming daartegen. Er waren afdelingen voor biochemie, farmacologie, radiobiofysica, fysica, microbiologie, celbiologie, genetica van micro-organismen en neurofarmacologie (Hoeneveld, 2018).

Een typische eigenschap van de Nederlandse militaire kennisinfrastructuur is dat de verbondenheid met de civiele kennisinfrastructuur altijd is blijven bestaan. De meeste betrokken partijen, zoals TNO, MARIN en NLR, zijn niet puur militair en hebben allemaal ook een civiele tak, die groter is dan de militaire tak. Die integratie is bijzonder. In de meeste andere westerse landen is gekozen voor een andere structuur en valt het defensieonderzoek direct onder het ministerie van Defensie (Lintsen, 2012).

Die integratie uit zich op verschillende manieren. In de eerste plaats door het klassieke *spillovereffect* van defensieonderzoek naar het civiele domein. Ook in Nederland komt dit regelmatig voor, bijvoorbeeld bij ergonomieonderzoek, audiologisch onderzoek en verkeersveiligheid. Maar interactie vindt ook op subtielere wijze plaats, al tijdens het onderzoeksproces. Zo wordt de defensietak van TNO regelmatig benaderd door civiele onderdelen van TNO. Andersom vindt ook kruisbestuiving plaats. Het verfinstituut van TNO wordt bijvoorbeeld betrokken bij onderzoek naar coatings voor marineschepen, het metaalinstituut van TNO voor onderzoek naar de betrouwbaarheid van lasnaden, en voedingsonderzoek door TNO wordt gecombineerd met onderzoek naar de kwaliteit van nood- en gevechtsrantsoenen (Lintsen, 2012).

2.2.2 Rol van wetenschappelijke instituten

Wetenschappelijke instituten zijn organisaties die onderdeel uitmaken van de academische gemeenschap, maar niet tot de groep universiteiten behoren. Zij hebben uitsluitend een onderzoekstaak en richten zich op een specifiek vakgebied. In Nederland zijn deze instituten georganiseerd binnen de KNAW en de NWO.

Tot 2017 viel een deel van deze wetenschappelijke instituten onder het FOM, de Stichting voor Fundamenteel Onderzoek der Materie. In 2017 is FOM opgegaan in NWO en zijn de vier nog bestaande FOM-instituten nu NWO-instituten geworden.[3]

[3] Deze vier instuten zijn ARCNL (Advanced Research Center for Nanolithography), Nikhef (Nationaal instituut voor subatomaire fysica), AMOLF (Instituut voor Atoom- en Molecuulfysica) en DIFFER (Dutch Institute for Fundamental Energy Research).

De oprichting van het FOM was, net als de oprichting van de Rijksverdedigingsorganisatie TNO, in 1946. Een belangrijke aanleiding voor de oprichting van FOM was het besef over wat de atoombommen van augustus 1945 teweegbrachten. Hiermee werden de enorme militaire én potentiële economische implicaties van de ontwikkelingen in deze nieuwe kernenergie direct duidelijk, evenals het feit dat de VS een enorme voorsprong had genomen op dit terrein. Ook was duidelijk dat deze bommen waren ontwikkeld in wetenschappelijke laboratoria en dat fundamentele wetenschappelijke kennis dus de basis was geweest. Hoeneveld (2018) stelt dan ook dat de belangstelling voor fysisch en nucleair onderzoek in Nederland niet los kan worden gezien van het vallen van de atoombommen en het besef dat wetenschap en oorlog nu voorgoed met elkaar verbonden waren.

Overigens was het niet de insteek om als reactie zelf een atoombom te gaan ontwikkelen. Al in de eerste voorbereidende vergadering van 3 november 1945 kwam expliciet aan de orde dat FOM duidelijk moest maken dat Nederland op geen enkele manier dacht aan gebruik van de kernenergie voor defensiedoeleinden. Nederlands kernfysisch onderzoek is (waarschijnlijk) nooit gericht geweest op militaire toepassingen. Met de naam 'Onderzoek der Materie' kozen de oprichters voor het uitdagen van een brede visie: naast (kern)fysica wilden zij ook een brug slaan naar materiaalwetenschap, chemie en andere disciplines (Hoeneveld, 2018).

Een interessante anekdote is dat de toenmalige minister de Leeuw van OKW (Onderwijs, Kunsten en Wetenschappen) zich zorgen maakte over het feit dat de kernenergiediscussie als gevolg had dat het overgrote deel van het budget voor wetenschap naar de fundamentele fysica ging. De minister was van mening dat de wetenschap zich niet op de juiste wijze zou kunnen ontwikkelen als de alfawetenschappen verwaarloosd zouden worden. Hij merkte op dat men ook in de Verenigde Staten inzag dat niet alleen de natuurwetenschappen moesten worden gestimuleerd, en stelde: ‘Men mag bij de destructieve neigingen van de beta-afdeeling, van de alpha vakken een zeker tegenwicht verwachten’ *(*ibid*)*.

2.2.3 Rol van Nederlandse universiteiten

Zoals we lieten zien, spelen verschillende wetenschappelijke disciplines een belangrijke rol in de Nederlandse militaire kennisecosystemen. Wat echter opvalt is dat het militaire onderzoek in Nederland meer gescheiden is van de universitaire instellingen dan in bijvoorbeeld de Verenigde Staten en het Verenigd Koninkrijk. Daar kenden universiteiten zoals Johns Hopkins en Imperial College London altijd nauwe banden met het ministerie van defensie en de defensie-industrie (Smart, 2016).

Nederlandse universiteiten doen van oudsher vrijwel geen militair onderzoek in opdracht van of in samenwerking met Defensie (Gummett & Stein, 1997; Cops, 2018).

Dat wil niet zeggen dat er helemaal geen defensie-gerelateerd onderzoek werd gedaan. De banden tussen universiteiten en Nederlandse industriepartners, zoals met het Philips Natlab en Holland Signaal, waren in sommige gevallen hecht - en zijn dat nog steeds. De samenwerking tussen Holland Signaal, het huidige Thales Nederland, en de Universiteit Twente is wellicht het bekendste voorbeeld. Deze samenwerking bestaat al sinds de oprichting van de universiteit in 1961 (de Boer, 2011).

Over het algemeen ligt onderzoek van universiteiten voor militaire doeleinden in Nederland historisch gevoelig. Zo werd al in 1946 het Verbond van Wetenschappelijke Onderzoekers (VWO) opgericht, dat zich verzette tegen een steeds hechtere relatie tussen wetenschap en defensie. Alleen door middel van verantwoordelijke interventies, zo meenden zij, kon een wereldwijde nucleaire wapenloop en daarmee een waarschijnlijke mondiale catastrofe worden voorkomen. Een voorstel begin jaren ‘50 om, naar Amerikaans voorbeeld, de steeds hogere defensiebudgetten deels voor wetenschappelijk onderzoek in te zetten, viel in wetenschappelijke kringen bijzonder slecht.

Eind jaren zestig nemen de maatschappelijke discussies over defensiegerelateerd onderzoek toe. Ook vanuit de journalistiek en talloze maatschappelijke bewegingen kwam verzet tegen het ‘militair-industrieel-wetenschappelijk complex’. Dit leidde begin jaren ‘80 tot een brede maatschappelijke steun voor een neutrale opstelling van Nederland, de zogenaamde 'Hollanditis'. Deze term werd in 1981 geïntroduceerd door de Amerikaanse historicus Walter Laqueur. Hij zag in het ontstaan van dit 'virus' in Nederland een hernieuwd neutralisme en 'a desire to keep out of world problems and an aversion to spend money on defense' (Hoeneveld, 2018). Een goed voorbeeld van de maatschappelijke discussie binnen universiteiten, is de interne strijd bij de Universiteit Twente. Daar kwam in de jaren ‘80 de afdelingsraad van de faculteit Elektrotechniek in conflict met het College van Bestuur over de vraag of college mocht worden gegeven aan werknemers van Holland Signaal (de Boer, 2011).

2.3 Afwegingskaders en procedures voor onderzoek dat raakt aan defensie en veiligheid

Met de groeiende aandacht voor defensieonderzoek na de Tweede Wereldoorlog wordt het belang van wetenschappelijk onderzoek voor defensiedoeleinden evident.

Een gevolg hiervan was dat strikte geheimhouding een belangrijk aspect van defensieonderzoek werd. Zo leidde de *Atomic Energy Act* van 1946 in de VS tot de ‘born secret’ doctrine, die stelt dat bij voorbaat alle informatie met betrekking tot de werking van kernwapens geheim is – en dit dus niet eerst geëvalueerd hoeft te worden (Morland, 2005). Ook de oprichting van de Rijksverdedigingsorganisatie TNO is deels te verklaren door de noodzaak tot geheimhouding en het feit dat Nederlandse universiteiten vaak geen geheim onderzoek aanvaarden. Binnen de Rijksverdedigingsorganisatie kon Nederlands defensieonderzoek wel onder strikte geheimhouding plaatsvinden (Lintsen, 2012).

Naast geheimhouding namen landen verschillende maatregelen om te voorkomen dat gevoelige of strategische kennis in handen kwam van verkeerde partijen. Deze maatregelen hingen altijd samen met de op dat moment relevante *state-of-the-art* kennis, en de dan geldende geopolitieke spanningen. Kenmerkend voor de naoorlogse periode was fundamentele natuurkundige kennis in de context van de Koude Oorlog. Zo ging er in de VS een lijst rond met vooraanstaande Europese natuurkundigen, waaronder ook een aantal Nederlanders, die bij een aanval van de Russen direct geëvacueerd moesten worden naar de VS (Hoeneveld, 2018). Naast kennis op het gebied van nucleaire fysica werd ook biologische en chemische kennis snel als risicogroep geclassificeerd. Vaak worden deze vakgebieden samengevoegd onder de afkorting BCRN (Biologisch, Chemisch, Radioactief en Nucleair).

Maatregelen schoten soms tekort, en incidenten leidden vaak tot verdere aanscherping. Een berucht voorbeeld waarbij het ‘goed mis’ ging, is het Nederlandse Urenco-schandaal. In de jaren zeventig wist de Pakistaanse atoomgeleerde Abdul Khan als spion bij Urenco geheime nucleaire kennis te vergaren over uraniumverrijking. Kennis die hij meenam naar zijn geboorteland, waar hij als 'de vader van het Pakistaanse kernprogramma' wordt gezien. Pakistan bracht in 1998 voor het eerst een atoombom tot ontploffing. Volgens inlichtingendiensten verkocht Khan ook nucleaire technologie aan onder meer Noord-Korea, Libië en Iran (Hosselet & Schuyffel, 2014).

Nieuwe geopolitieke spanningen zorgen ook continu voor een evaluatie van bestaande protocollen. De terroristische aanslag van 11 september 2001 en de snel daarop volgende (overigens niet gerelateerde) Anthrax-brieven leidden in Amerika bijvoorbeeld tot diverse nieuwe voorschriften of versterkte handhaving van bestaande voorschriften, met name op het gebied van biomedisch onderzoek (Reich, 2011). Maar ook screening van en controle op buitenlandse studenten in het algemeen nam toe, omdat politici vermoedden dat terroristen met een

studentenvisum de VS binnen zouden zijn gekomen[4]. Ook in Nederland leidden de Anthrax-brieven tot een politieke reactie, en uiteindelijk tot een KNAW-*code of conduct* voor biosecurity (KNAW, 2008).

Door de jaren heen is er een systeem opgetuigd rondom *dual-use* wetgeving, exportcontrole, sancties en kennisembargo's. Deze maatregelen werden ingepast binnen een internationaal raamwerk van internationale verdragen en resoluties, en zowel nationale als Europese wet- en regelgeving. Zonder een totaaloverzicht te willen geven, illustreren we hier in grote lijnen hoe Nederlands onderzoek zich moet verhouden tot specifieke instituties.

Internationale verdragen en afspraken

Ten eerste zijn er in de loop der tijd verschillende multilaterale verdragen tot stand gekomen voor de controle van export. De eerste hiervan, de *Nuclear Suppliers Group*, stamt uit 1974 en bestaat uit een groep landen die nucleaire proliferatie probeert te voorkomen door controle uit te oefenen op de export van materialen, apparatuur en technologie die kunnen worden gebruikt voor de productie van kernwapens.

De *Missile Technology Control Regime* stamt uit de jaren '80 van de vorige eeuw en had als doel om de verspreiding van raketten en rakettechnologie te beperken. Ook uit de jaren '80 stamt de *Australia Group*, een exportcontrole-regeling die lidstaten moet helpen om exporten te identificeren die kunnen bijdragen aan de verspreiding van chemische en biologische wapens.

Het laatste multilaterale verdrag voor de controle van export werd gesloten in 1996. Het *Wassenaar Arrangement* (voluit *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*) is een akkoord over de beperking van de export van conventionele wapens en van technologieën die ook voor militaire doeleinden kunnen worden gebruikt.

EU *dual-use* verordening

De bepalingen in deze internationale bronnen zijn in de aangesloten landen nader uitgewerkt in eigen wetten en regels. Voor Nederland speelt de EU hierin een belangrijke rol. Zo stelt de Europese dual-use verordening dat een organisatie een vergunning nodig heeft voor export naar landen buiten de Europese Unie (EU), en voor de overdracht van sommige gevoelige dual-use goederen (d.w.z. met zowel een civiele als militaire toepassing) binnen Europa. Voor de exportcontroles gebruikt de Nederlandse overheid dan ook de Europese lijst voor dual-use goederen. De focus van deze lijst ligt op goederen die kunnen bijdragen aan de

4 Uiteindelijk bleek overigens dat maar 1 van de 19 vliegtuigkapers de VS binnen was gekomen op een studentenvisum. https://www.factcheck.org/2013/05/911-hijackers-and-student-visas/

productie of verspreiding van massavernietigingswapens. Dit zijn bijvoorbeeld kernwapens, chemische strijdgassen of biologische wapens. Het ministerie van Buitenlandse Zaken is eindverantwoordelijk voor beleid en implementatie. Uitvoering ligt in principe bij het centraal loket voor vergunningaanvragen van de Douane, maar complexere of politiek gevoelige dossiers worden door het ministerie zelf behandeld.

Exportvergunningen kunnen ook van toepassing zijn voor wetenschappers die potentieel gevaarlijk onderzoek elders willen publiceren. Een goed voorbeeld hiervan is de zaak rondom de Nederlandse hoogleraar Virologie Ron Fouchier, die er in 2011 in slaagde een levensgevaarlijke variant van de vogelgriep in elkaar te zetten. Fouchier stuurde een artikel met zijn bevindingen naar vakblad *Science*, waarna wereldwijde commotie ontstond. Publicatie werd uit veiligheidsoogpunt lang tegengehouden. De angst bestond dat de informatie zou worden misbruikt door bioterroristen. De Nederlandse overheid besloot dat een exportvergunning in deze gevallen noodzakelijk is.

Kennisembargo's

Vanuit de VN, EU of nationale overwegingen kunnen ook handelsbeperkende maatregelen worden afgeroepen, zoals de VNVR-resoluties 1874 tegen Noord-Korea en resolutie 1737 tegen Iran. Op basis van deze verdragen kunnen sancties worden uitgesproken. Dit zijn tijdelijke verboden op het ter beschikking stellen van economische middelen aan 'geliste' entiteiten. Dit kan zowel een land, een regio, een organisatie of een persoon zijn.

Wetenschappelijke samenwerking kan hier ook onder vallen. Op dit moment geldt een dergelijk kennisembargo alleen voor Noord-Korea, maar het kabinet wil het scherpere toezicht uitbreiden tot meer landen. Dat toezicht richt zich in de eerste plaats op studenten en onderzoekers uit Iran. Op die manier moet worden voorkomen dat specialistische, in Nederland opgedane kennis, kan worden gebruikt voor het ontwikkelen van wapens in Iran. Uitsluiten op basis van nationaliteit is een gevoelig onderwerp. Eerdere pogingen van de overheid om onderzoekers op basis van nationaliteit toegang te ontnemen tot specifieke locaties waar gevoelig onderzoek wordt uitgevoerd, is na aanvechting door universiteiten door het Hooggerechtshof teruggedraaid (KNAW, 2014). Het kabinet verwacht voor het besluit over Iran wel voldoende juridische gronden te hebben en sluit niet uit dat in de toekomst mogelijk ook studenten met banden met andere risicolanden extra in de gaten worden gehouden (Ministerie van Buitenlandse Zaken, 2019).

Kortom, de afgelopen decennia is een palet aan afwegingskaders en procedures opgesteld voor onderzoek dat raakt aan defensie en veiligheid. Het gaat hier veelal om biologisch, chemisch, radioactief en nucleair (BCRN) onderzoek op hogere

TRL's (technology readiness levels), te herkennen als *dual-use*. Deze regels bepalen dat er verscherpte procedures moeten worden gevolgd indien speur- en ontwikkelwerk naast een civiele, mogelijk ook een militaire toepassing oplevert. Met specifieke aandacht voor toepassingen waarmee schade kan worden toegebracht. In dat geval gelden beperkingen ten aanzien van de manier waarop informatie en kennis gedeeld mogen worden, met wie mag worden samengewerkt en wat er aan resultaten wel of niet de grens over mag. Wanneer onderzoek en ontwikkelwerk tot een product leiden, is er een exportvergunning vereist.

2.4 Een nieuwe dynamiek in kennisecosystemen

Na de wapenwedloop tijdens de Koude Oorlog brak er een tijd aan waarin relatief minder aandacht uitging naar kennisontwikkeling voor defensie en veiligheid. Het wegvallen van de urgentie van de Koude Oorlog leidt vrijwel overal ter wereld tot een daling in uitgaven aan defensie en defensiegerelateerde R&D.

In hoofdstuk 1 lieten we zien dat er momenteel hernieuwde aandacht voor is, waarbij digitalisering kan worden gezien als een *gamechanger*: Digitalisering leidt tot tal van nieuwe innovaties in het militaire domein, en creëert met 'cyber' naast land, zee, lucht en ruimte een nieuw domein voor conflict.

In deze paragraaf laten we zien dat digitalisering zorgt voor een andere dynamiek in het kennisecosysteem. De kennisontwikkeling voor de wapenwedloop tijdens de Koude Oorlog kreeg hoofdzakelijk vorm binnen militaire en nationaal aangestuurde/georganiseerde kennisecosystemen. Bij de huidige digitale wapenwedloop speelt kennisontwikkeling in het civiele domein een grote rol, en wordt deze kennis ontwikkeld in mondiaal vervlochten kennisecosystemen. We lichten deze punten hieronder toe.

2.4.1 Het belang van civiele kennisontwikkeling voor defensie en veiligheid

Civiele kennisontwikkeling als bron voor militaire innovatie
Met de digitale wapenwedloop neemt het belang van civiele kennisontwikkeling voor defensie en veiligheid toe. Defensie is op veel domeinen niet langer meer de vernieuwer. Veel digitale militaire innovaties bouwen voort op een kennisbasis die van oorsprong met civiele doeleinden werd ontwikkeld. Om een militair overwicht te

behouden of te verkrijgen zijn landen daardoor afhankelijk van kennis van universiteiten en bedrijven uit het civiele domein.

Denk aan de belangrijke rol van het cluster techbedrijven en kennisinstellingen rondom ‘Silicon Valley’, die steeds meer de drijvende kracht vormt achter nieuwe kennis en innovatie. De techgiganten investeren grote bedragen in R&D. Met name op gebied van robotica en kunstmatige intelligentie zijn dit bedrijven die de innovaties van de toekomst vormgeven. Zo besteden bedrijven als Uber en Waymo, het dochterbedrijf van Google, honderden miljoenen euro’s aan R&D voor zelfrijdende auto’s, en rijden zij rond met duizenden testauto’s om deze technologie verder te ontwikkelen. Ook Chinese techgiganten zoals Alibaba, Huawei en Baidu spelen een belangrijke rol in het vormgeven van onze digitale samenleving. Hoewel Europa niet over uitgesproken techgiganten beschikt, vindt ook hier veel kennisontwikkeling plaats binnen bedrijven die diensten en producten leveren op de civiele markt – denk in Nederland bijvoorbeeld aan bedrijven als ASML, Philips en NXP. Deze bedrijven bouwen op een uitgebreid ecosysteem van midden- en kleinbedrijf, en werken vaak intensief samen met universiteiten in nieuwe vormen van publiek-private samenwerking.

De relatie tussen militaire en civiele R&D is daarom niet meer enkel een van ‘spin-offs’, maar ook van ‘spin-ins’ (James, 2009). Immers, Defensie heeft niet de capaciteiten om de kennisbasis voor een moderne krijgsmacht volledig ‘intern’ te kunnen afdekken. De focus verschuift van zelf technologie ontwikkelen naar het overnemen van civiele innovaties en het aanpassen van deze innovaties aan een militaire context. Dit betekent dat vernieuwing niet meer automatisch uit het vertrouwde militaire kennisecosysteem komt. In plaats daarvan gaan actoren die verantwoordelijk zijn voor militaire kennisontwikkeling actief op zoek naar nieuwe relaties in het kennisecosysteem. Bijvoorbeeld door directer aan te haken op kennis die wordt ontwikkeld op universiteiten, of door meer samen te werken met bedrijven uit de civiele sector, van multinational tot startup. De civiele kennisinfrastructuur wordt dus regelmatig gemobiliseerd voor defensie- en veiligheidsdoeleinden.

Een veelgenoemd voorbeeld uit de VS is initiatief DIUx (Defence Innovation Unit Experimental). DUIx heeft als doel samenwerking uit te lokken met *Silicon Valley* en gaat via investeringen partnerschappen aan met kleine innovatieve technologiebedrijven die voorheen niet in aanraking kwamen met defensie. De focus ligt op het gebied van robotica, kunstmatige intelligentie en big data-analyse (Seligman, 2018). DUIx heeft sinds 2016 zo’n 100 miljoen dollar gestoken in 45 projecten. In verhouding met het totale R&D-budget van 77 miljard USD in 2016, is het budget van DUIx klein, maar het lijkt te kunnen rekenen op steun en groei (Simonite, 2017).

In Nederland realiseerde het ministerie van Defensie zich eveneens dat het zonder inschakeling van de civiele sector moeilijk tot innovatie komt. Het uitgangspunt van de nieuwe innovatiestrategie van Defensie '*samen sneller innoveren'* is dat het ministerie tijdig moet kunnen inspelen op de kansen en mogelijkheden voor het verbeteren van zijn operationeel effect die ontwikkelingen in de samenleving, technologie en wetenschap bieden. De innovatiestrategie is een leidraad voor hoe Defensie beter en sneller innovaties kan absorberen. Hierbij gaat het expliciet niet alleen om technologische innovaties, maar ook om tal van sociale en organisatorische innovaties en de daarmee gepaard gaande culturele veranderingen. De focus ligt sterk op de rol van mensen, het creëren van ruimte voor experiment, het stimuleren van de juiste *mindset* en nieuwe manieren van denken, en op samenwerking in multidisciplinaire teams van partijen binnen en buiten defensie.

Zo is het Nederlandse ministerie van Defensie een soortgelijk initiatief gestart als het Amerikaanse DUIx, te weten FRONT - wat staat *voor Future Relevant Operations with Next generation Technology*. FRONT wil verbinding zoeken met startups, onder meer door samenwerking met startup-incubators bij universiteiten, zoals YES! Delft van de TU Delft.

Ook voert Defensie samen met een aantal andere partijen een onderzoek uit naar de opzet, vorm en organisatie van een in 2019 op te richten Cyber Innovation Hub, waarin departementen, onderzoeksinstellingen en bedrijven samen werken aan gezamenlijke en geprioriteerde veiligheidsvraagstukken op het gebied van cyber(security). Het doel van de Cyber Innovation Hub is cyberkennis en -kunde in Nederland versterken, innovaties en experimenten faciliteren en een ecosysteem van partners bouwen, om zo bij te dragen aan het reduceren van cyberdreigingen.

Ten slotte gaat het ministerie van Defensie werken met een *Chief Scientific Advisor* (CSA) en een *Chief Innovation Advisor* (CIA). De CSA treedt op als intermediair tussen de (internationale) academische wereld en Defensie om alle partijen vroegtijdig te betrekken bij nieuwe ontwikkelingen. Deze rol zal worden ondergebracht bij de decaan van de faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie (NLDA).

De *Chief Innovation Advisor* is aanjager van het innovatienetwerk bestaande uit diverse 'innovatiekolonels' die innovatie moeten versterken binnen de verschillende afdelingen van de krijgsmacht. De CIA moet samenwerking en samenhang bevorderen en geeft direct advies aan de defensietop. Deze rol zal worden ondergebracht bij FRONT, als onderdeel van de Defensiestaf.

Civiele kennisontwikkeling als risico voor defensie en veiligheid
De actoren die zich bezighouden met de ontwikkeling van digitale technologieën doen dit doorgaans met een civiel doel voor ogen: de aanleg van betere communicatienetwerken, het aansluiten van apparaten op het internet voor efficiëntere industriële processen of betere dienstverlening en het verbinden van mensen via digitale platforms. Maar ook de civiele innovaties kunnen leiden tot nieuwe kwetsbaarheden op het gebied van defensie en veiligheid: nieuwe communicatienetwerken kunnen worden gebruikt voor spionage, het aansluiten van miljarden apparaten op het internet der dingen creëert een groot veiligheidsrisico en *social media* spelen een belangrijke rol in de verspreiding van nepnieuws. Als gevolg hiervan worden kennisinstellingen en bedrijven die zich primair op de civiele markt richten, nu steeds vaker vanuit een defensie- en veiligheidsperspectief beschouwd.

De komende jaren staan in het teken van tal van digitaliseringsprocessen die de fysieke wereld en het cyberdomein steeds inniger met elkaar verbinden. Denk aan de uitrol van het 5G-netwerk of de introductie van de zelfrijdende auto. Kennisinstellingen zullen hier een belangrijke rol in spelen. Van kennisinstellingen wordt steeds vaker verwacht dat defensie- en veiligheidsaspecten geen *afterthought* zijn. De nieuwe kwetsbaarheden van de digitale samenleving leiden tot de oproep om meer structurele oplossingen voor dergelijke problemen te ontwikkelen, waardoor steeds vaker wordt geëist dat defensie- en veiligheidsaspecten een standaard onderdeel zijn van de beoordeling van onderzoeksprocessen – van voorstel tot evaluatie. Zo heeft de Britse overheid in 2018 als eerste land uitgebreide cybersecuritystandaarden opgesteld voor zelfrijdende auto’s (Department of Transport, 2018).

2.4.2 Het internationale karakter van kennis en innovatie

Internationale samenwerking
Anders dan de nationaal georganiseerde militaire kennisecosystemen van voorheen, kenmerkt kennisontwikkeling in deze digitale wapenwedloop zich door een uitgesproken internationale dynamiek. Kennisontwikkeling is tegenwoordig praktisch ondenkbaar zonder internationale samenwerking. Mondialisering veranderde de manier waarop bedrijven hun producten en diensten ontwikkelen, produceren en op de markt brengen. Mondialisering betekent ook dat activiteiten die vroeger in één bedrijf zaten, nu verdeeld worden over meerdere bedrijven en landen. Deze fragmentatie van waardeketens leidt tot complexe arbeidsdelingen tussen toeleveranciers en producenten in verschillende landen, waarbij open innovatiestrategieën worden gevolgd waarin ze samenwerken met externe kennispartners wereldwijd (Deuten, 2014).

Rondom digitalisering komt deze internationale component nog nadrukkelijker naar voren. Digitale kennisecosystemen hebben een mondiaal karakter, zoals symbolisch staat verwoord op de achterkant van elke iPhone: *Designed by Apple in California. Assembled in China.* Een van de belangrijkste sectoren in de digitale wapenwedloop, de chipindustrie, kent ook een Nederlandse actor. ASML is als de belangrijkste leverancier van machines voor de halfgeleiderindustrie een centrale speler in een internationaal vervlochten kennisecosysteem.

In de digitale wapenwedloop is kennisontwikkeling voor defensie en veiligheid ondenkbaar zonder internationale samenwerking. Nederland is niet in staat om volledig zelfstandig een straaljager te bouwen, laat staan een kwantumcomputer. Het idee dat elk land een eigen *defence-industrial base* nodig heeft is door veel, met name kleinere, landen losgelaten.

Nederland werkt via verschillende routes in internationaal verband samen op het gebied van onderzoek en innovatie voor defensie en veiligheid. Zo werkt Nederland bilateraal samen met Noorwegen op het terrein van chemische, biologische en radioactieve stoffen (CBRN), en wordt samengewerkt binnen de *NATO Technology Programmes*. Recent is ook de EU zich steeds nadrukkelijker aan het manifesteren als platform voor samenwerking voor kennis en innovatie gericht op defensie en veiligheid (Europese Commissie, 2017).

Internationale spanningen

De afgelopen jaren zien we dat internationale samenwerking onder druk komt te staan. Overheden, bedrijven en universiteiten besluiten samenwerking met bepaalde landen of organisaties te boycotten. Nationale veiligheid is vaak een belangrijk onderdeel van de afweging. Met name Amerika en China lijken verwikkeld te raken in wat ook wel geduid wordt als een ‘technologische koude oorlog’ (Vervaeke, 2019).

Illustratief is de recente ontwikkeling rondom de rol van het Chinese Huawei in de uitrol van het nieuwe 5G-netwerk. Deze civiele technologie wordt steeds meer beschouwd vanuit een perspectief van nationale veiligheid. Zo waarschuwt de VS voor spionage, aangezien Huawei achterdeurtjes zou inbouwen om de Chinese overheid te faciliteren in cyberspionage. De VS roepen andere landen dan ook op om niet samen te werken met Huawei; iets waar Australië en Nieuw-Zeeland gehoor aan lijken te geven. Europese landen lijken vooralsnog een eigenstandige koers te varen, en gaan wel (deels) in zee met Huawei als partner in de aanleg van 5G-netwerken. Hoewel van een gezamenlijke Europese strategie vooralsnog geen sprake lijkt (Pelgrim 2019). De Huawei-casus laat ook zien hoe economische, politieke en militaire doelen door elkaar heen lopen. Bewijs voor achterdeurtjes is vooralsnog niet gevonden – of in ieder geval niet openbaar gemaakt, wat vragen

oproept over de achterliggende motieven in deze technologische koude oorlog (Johnson & Groll, 2019).[5]

Deze nieuwe *technopolitiek* leidt niet alleen tot spanningen met verre landen, maar is ook een *issue* tussen buurlanden en bondgenoten. Een goed voorbeeld is een brandbrief op het gebied van cybersecurity van vooraanstaande Nederlandse wetenschappers uit oktober 2017, die stellen dat Duitsland kennis op cybersecurity weghaalt uit Nederland (Bos et al., 2017).

Deze internationale spanningen beperken zich niet tot afwegingen over technologie, maar werken ook door voor de mensen die kennis hebben over deze technologie. Verschillende partijen waarschuwen voor de rol van internationale mobiliteit van studenten en onderzoekers en het gevaar voor wat ook wel *deemed export* wordt genoemd: het exporteren van gevoelige informatie doordat kennis terechtkomt bij personen uit een ander land, bijvoorbeeld via onderwijs of participatie in onderzoek. Hiervoor hoeft een bepaalde technologie het land niet te verlaten, aangezien de onderzoeker de kennis mee kan nemen naar zijn of haar thuisland.

Nederland is bepaald niet onbekend met deze problematiek. Een illuster voorbeeld dat we eerder al bespraken, is Abdul Qadir Kahn, de ‘vader van de Pakistaanse atoombom’. Hij wist essentiële kennis op dit gebied te vergaren tijdens zijn werkzaamheden voor Urenco in Almelo. In de VS is voor zulke situaties wetgeving ontwikkeld. Als gereguleerde informatie of technologie wordt vrijgegeven aan een in de Verenigde Staten woonachtige vreemdeling, wordt dit beschouwd als een export naar het thuisland of de landen van de buitenlandse staatsburger (Bureau of Industry and Security, 2016). In de huidige EU wetgeving over dual-use is dit niet meegenomen en ontbreekt een duidelijk afwegingskader rondom dit soort problematiek.

2.5 Conclusie

Het doel van dit hoofdstuk was om de huidige ontwikkelingen in een historisch perspectief te plaatsen en de vraag te beantwoorden wat de verschillen zijn tussen de historische en huidige kennis- en innovatieagenda’s voor defensie en veiligheid. We lieten zien dat na de Tweede Wereldoorlog kennisontwikkeling voor defensie en veiligheid werd georganiseerd in militaire kennisecosystemen, met duidelijke grenzen tussen militaire en civiele kennisecosystemen.

5 Wel publiceert de Volkskrant op 16 mei 2019 een bericht over een vermoeden dat Huawei over een verborgen achterdeur naar klantgegevens van een van de grote Nederlandse telecomproviders beschikt en daarmee betrokken is bij Chinese spionage. De AIVD zou er onderzoek naar doen.

De meeste spelers uit de publieke kennisinfrastructuur lieten zich niet in met onderzoek voor militaire doeleinden.

Ook in Nederland ontstond na WOII een militair kennisecosysteem. De Rijksverdedigingsorganisatie van TNO, later TNO Defensie & Veiligheid, speelt een centrale rol. Ook de oprichting van FOM kan niet los worden gezien van de zowel economische als militaire strategische waarde van fundamenteel kernfysisch onderzoek. Nederlandse universiteiten houden, met uitzonderingen daargelaten, gepaste afstand van defensieonderzoek. In de loop der tijd ontstaan er diverse maatregelen en procedures voor onderzoek dat raakt aan defensie en veiligheid. Dual-use werd het leidende afwegingskader.

De huidige context kenmerkt zich door een vervaging van het onderscheid tussen civiele en militaire kennisontwikkeling. Met name digitalisering leidt ertoe dat het onderscheid tussen een civiele en een militaire kennisinfrastructuur steeds lastiger te maken is – en dat de civiele structuur zich dus steeds meer bewust moet zijn van de mogelijke consequenties van onderzoek en innovatie voor veiligheid.

Daarnaast is er sprake van het internationaliseren van kennisontwikkeling en innovatie in het algemeen, en van die gericht op defensie en veiligheid in het bijzonder. Anders dan de nationaal georganiseerde militaire kennisecosystemen van voorheen, kenmerkt kennisontwikkeling in deze digitale wapenwedloop zich door een uitgesproken internationale dynamiek. Dit biedt kansen voor samenwerking, maar veranderende internationale verhoudingen leiden ook tot spanningen rondom (gezamenlijke) kennisontwikkeling.

3 Casestudy: maritiem domein

In deze casestudy hebben we gekozen voor een focus op het maritieme domein omdat Nederland van oudsher een sterke maritieme defensiesector kent. Momenteel is dit het enige domein waarbinnen Nederland beschikt over een goede kennisbasis en een significante industrie. Ook is Defensie van plan een groot deel van de Nederlandse vloot binnenkort te vernieuwen. De komende jaren staan in het teken van de vervanging van onder meer onderzeeboten, fregatten en mijnenjagers. Dit brengt allerlei keuzes en dilemma's aan het licht die illustratief zijn voor de huidige dynamiek van kennis en innovatie voor defensie en veiligheid.

Voor deze casestudy voerden we deskresearch uit en hielden we interviews met experts uit de sector. Om een zo volledig mogelijk beeld te krijgen, spraken we met deskundige vanuit de overheid (ministerie van Defensie), het bedrijfsleven (Damen Shipyards en Thales Nederland), brancheorganisaties (Nederland Maritiem Land), universiteiten (TU Delft) en publieke kennisinstellingen (TNO en MARIN).

3.1 Nieuwe kennis- en innovatieagenda's voor de marine

De veranderende veiligheidssituatie, zoals beschreven in hoofdstuk 2, heeft ook implicaties voor de rol van de krijgsmacht op zee. In het maritieme domein staan zelden twee landen met twee vloten tegenover elkaar. Meestal is er sprake van een confrontatie tussen zeer verschillende actoren met uiteenlopende strategieën. Zo is de Nederlandse marine steeds meer actief in asymmetrische conflicten met bijvoorbeeld drugssmokkelaars of piraten. Dit vraagt om modulaire, flexibele schepen passend bij de diverse missies en doelen (HCSS, 2016).

Daarnaast is *flow security* een belangrijke taak geworden van de Marine. *Flow security* refereert naar het beschermen van alle '*flows*' waarop moderne samenlevingen bouwen. Dit betreft niet alleen handelsroutes, maar ook andere *flows* die zich (deels) op of onder water bevinden: energienetwerken, internetkabels, etc. Veel van onze data- en stroomkabels liggen op de zeebodem en zijn praktisch onverdedigd (WRR, 2018). Een kwaadwillende kan met een ongezien vaartuig enorme schade aanrichten. Dit wordt ook wel *seabed warfare* genoemd. Maritieme surveillance wordt hierdoor een belangrijke taak.

In deze context is digitalisering ook bij de marine een belangrijke technologische ontwikkeling. Schepen functioneren steeds meer als drijvend data-, informatie- en coördinatiecentrum (van Huizen, 2017). De beschikbaarheid en verwerkingsmogelijkheden van grote hoeveelheden data door ontwikkelingen in sensor- en radartechnologie versnellen dit proces (Spoelstra, 2016). Een gevolg van de automatisering is dat minder bemanningsleden nodig zijn en hierdoor minder mensen gevaar lopen. Hoewel autonomie volop in ontwikkeling is, lijkt van volledige autonomie voorlopig nog geen sprake (Stam, 2017).

Het belang van digitalisering binnen de kennis- en innovatieagenda's in het maritieme domein komt ook duidelijk naar voren in de in april 2019 aangekondigde missies voor het topsectoren- en innovatiebeleid. Zes van deze 25 missies gaan over veiligheid, en één missie gaat specifiek over 'maritieme hightech voor een veilige zee'. Deze missie is verder uitgewerkt aan de hand van een stel kennis- en innovatievragen. In veel van die vragen speelt digitalisering een belangrijke rol. Zo wil de marine inzetten op onbemande en autonome middelen, AI en robotisering, *concept development* en experimenten in VR- en AR-omgevingen.

Ook hier is het goed te benadrukken dat digitalisering een belangrijke ontwikkeling is, maar niet de enige. Naast digitalisering is ook sprake van veel vernieuwing op het gebied van offensieve technologie, zoals steeds snellere en onvoorspelbaardere (intercontinentale) ballistische raketten en laserwapens (Freedberg, 2017). Ook blijft constante ontwikkeling op het gebied van sensortechnologie van strategisch belang. 'Vijandelijke objecten onder water detecteren is complexer dan objecten aan de oppervlakte of in de lucht, aangezien zeewater een veel moeilijker te doorgronden medium is vanwege verschillen in temperatuur, bodemcontouren en zoutgehalte' (van Baal, 2014). Sensor- en radartechnologie zijn continu in ontwikkeling, bijvoorbeeld voor de vroegtijdige waarneming van intercontinentale raketten, en voor detectie van onderwatergeluid om onderzeeboten op te sporen. Tegelijkertijd worden boten steeds stiller gemaakt en worden er coatings ontwikkeld om voertuigen minder herkenbaar te maken voor radar. Ook wordt in het kader van stillere boten gekeken naar de mogelijkheden van elektrisch varen.

3.2 Nederlandse traditie in maritieme kennisontwikkeling: de gouden driehoek

De marine is in Nederland van oudsher het onderdeel van de krijgsmacht dat de belangrijkste impulsen geeft tot innovatief onderzoek. De innovatiedynamiek in het marinebouwcluster kwam in het verleden voor een groot deel overeen met de

dynamiek van traditionele militaire kennisecosystemen zoals besproken in hoofdstuk 2.

De ontwikkeling van nieuwe schepen had van nature een lange cyclus, getrokken door grote defensieorders, en gekenmerkt door zwaar gejuridiseerde processen. Ten slotte kennen marineschepen hoge kwaliteits- en veiligheidseisen in vergelijking met de civiele vaart.

Marineschepen werden daarom ontwikkeld in de zogeheten ‘gouden driehoek’ van overheid, kennisinstellingen en een gespecialiseerde industrie, waarbinnen vertrouwde relaties en langdurige samenwerking tot stand konden komen. In onze interviews werd herhaaldelijk verwezen naar deze gouden driehoek, en werd benadrukt dat deze ook vandaag de dag nog van groot belang is. De gouden driehoek bestaat traditioneel uit onderstaande drie partijen.

- **De overheid** speelt een centrale rol middels het Ministerie van Defensie in de rol van behoeftesteller en eindgebruiker, en met het Ministerie van EZK dat verantwoordelijk is voor het betrekken van de Nederlandse industrie.
- **Kennisinstellingen,** met de publieke kennisorganisaties TNO en MARIN als centrale partijen, ontwikkelen kennis en verrichten toegepast onderzoek.
- **De industrie,** met een kern van drie bedrijven: Damen, RH Marine en Thales.

Na het trauma van de Walrus-affaire [6] nam de Nederlandse overheid een bescheidener rol op zich. Niet langer was het uitgangspunt om samen met ‘de gouden driehoek’ hele nieuwe boten te ontwikkelen. De doctrine verschoof van zelf ontwikkelen naar ‘van de plank’ kopen waar kan. Het nog overeind staande innovatiebeleid kwam voort uit een combinatie van economische belangen en de wens om toch ook een binnenlandse (technologische) kennisbasis te behouden (DeFrance et al., 2016).

In 2018 komt er een omslag in het beleid. De Defensienota 2018 en de daarop volgende Defensie Industrie Strategie 2018 laten een zelfverzekerde krijgsmacht zien die vooral wil inzetten op het versterken de kennis, technologie en industriële capaciteiten in het maritieme domein. Bij de vernieuwing van de vloot is ‘van de plank’ niet langer het devies, maar is de insteek om de eigen industrie voorrang te geven in het ontwerp en bouw van de nieuwe generatie schepen.

---

6 Eind jaren zeventig wordt besloten dat Nederland een volledig nieuwe duikbootklasse gaat ontwikkelen en bouwen, door Nederlandse partijen en in directe opdracht van de marine. Het budget wordt met 65% overschreden, iets wat de top van de marine lange tijd probeert te verzwijgen. Uiteindelijk wordt de volledige top vervangen en laat het trauma diepe sporen achter.

De bouw van deze nieuwe generatie schepen zal echter anders verlopen dan in het verleden. Ook in het maritieme domein is duidelijk sprake van een nieuwe innovatiedynamiek. De tijd van volledig nationaal georganiseerde defensie-industrieën ligt achter ons. Vier consortia dingen mee naar de opdracht voor de bouw van nieuwe onderzeeërs, voor een bedrag van circa 3,5 miljard euro: Damen Shipyards (Nederland) met Saab Kockums (Zweden), ThyssenKrupp Marine Systems (TKMS, Duitsland), Naval Group (Frankrijk) en Navantia (Spanje).
De Franse werf Naval heeft IHC als onderaannemer gestrikt en gooit daarmee naar verluidt hoge ogen (de Boer, 2019).

3.3 Een nieuwe dynamiek in het kennisecosysteem

3.3.1 Het belang van civiele kennis en innovatie

Traditionele militaire kennisecosystemen kenmerken zich door een duidelijke scheiding van het civiele kennisecosysteem. Bij het Nederlandse marinebouwcluster is dit onderscheid nooit zo absoluut geweest. Civiel-militaire integratie kwam altijd al voor. Er is nauwelijks sprake van partijen met een puur militaire of civiele missie. Dit geldt voor zowel kennisinstellingen TNO en MARIN, als voor industriepartners als Damen en RH Marine. Beide combineren civiele en militaire activiteiten binnen één organisatie. Hierin onderscheidt deze sector zich van de meer conventionele defensie-industrie.

Toch is het toenemend belang van civiele kennis en innovatie in het maritieme domein evident. Veel van de technologische ontwikkelingen, zoals in sensor- en radartechnologie, automatisering en ICT, komen niet meer uit militaire kennisecosystemen, maar bouwen voort op een van oorsprong civiele kennisbasis. Het belang van civiele kennis in het marinebouwcluster uit zich op twee manieren:

- Ontwikkelde kennis, maar ook de onderzoeksinfrastructuren en wetenschappelijke expertise die nodig zijn in het marinebouwcluster, zijn tot een vrij hoog TRL, *Technology Readiness Level*, generiek. Het onderscheid tussen militaire en civiele technologie ontstaat met name op meer toegepast niveau (hoog TRL).
- Het civiele domein kent een grote innovatiedynamiek. Op bepaalde technologische gebieden, bijvoorbeeld voor autonoom, stil en elektrisch varen, wordt de kennisbasis met name gevormd door grote civiele, en niet-militaire, investeringen in R&D. De kennis komt bijvoorbeeld van scheepswerven gespecialiseerd in luxejachten, binnenvaart of vrachtschepen, waar deze technologieën allemaal commercieel interessante toepassingen kennen. Dit is

ook goed zichtbaar in de Nederlandse industrie. Juist in jaren dat orders van defensie uitbleven, wisten deze partijen overeind te blijven door zich te richten op de civiele markt (Overgoor et al., 2018). Aangezien veel van die kennis overdraagbaar is, kan deze nu weer worden toegepast bij de vernieuwing van de Nederlandse vloot.

Als gevolg van deze ontwikkelingen wordt regelmatig een oproep gedaan tot 'nieuw denken' over innovatie binnen de marine. Bij dit nieuwe denken staat het toepassen van nieuwe technologieën uit het civiele domein in de militaire operatie centraal (Brouwer, 2015). De gedachte is dat wanneer de technologieontwikkeling met name vanuit het militaire domein komt, de marine kan bouwen op een lange geschiedenis van samenwerking binnen de gouden driehoek. Wanneer de technologieontwikkeling met name vanuit het civiele domein komt – iets wat dus steeds vaker het geval is – zou de marine op zoek moeten naar nieuwe relaties in het kennisecosysteem. Dit geldt in het bijzonder voor een aantal nieuwe sleuteltechnologieën, waarvan de verwachting is dat ze ook tot grote doorbraken in militaire capaciteiten zullen leiden (Ministerie van Defensie, 2016). De marine moet vanuit dit perspectief meer aansluiten bij de 'snelle innovatiecyclus' van partijen met een oorspronkelijk civiele missie.

Dit 'nieuwe denken' over innovatie vraagt om een nieuwe attitude. Het ministerie van Defensie probeert dan ook op verschillende manieren nieuwe verbindingen aan te gaan met het civiele kennisecosysteem. Zoals we in hoofdstuk 2 lieten zien, zijn er tal van initiatieven die dit willen bewerkstelligen. Startups en mkb (midden- en kleinbedrijf) worden hierin gezien als belangrijke partijen. Het ministerie van Defensie heeft diverse initiatieven opgezet om in aanraking te komen met nieuwe concepten vanuit het mkb, zonder de belemmeringen van traditionele aanbestedingsregels. Het idee is om als overheid een hybride omgeving te creëren en een innovatiecentrum op te zetten waar bedrijf en overheid kunnen samenwerken, zonder de grote hekken die civiel en militair traditioneel van elkaar scheiden.

Van 'gouden driehoek' naar 'gouden ecosysteem'

Toch benadrukken onze gesprekspartners dat het maritieme domein deels een traditioneel militair domein blijft, met een duidelijk verschil tussen een marineschip en een plezierjacht. Er is geen sprake van volledige integratie van civiele en militaire technologische ontwikkeling. Hoewel het verschil tussen militaire en civiele technologie pas op het niveau van de toepassing ontstaat, is dat geen lichte stap. Civiele technologie is niet zomaar militair inzetbaar. Een voorbeeld is de vaak gehoorde roep om het inzetten van drones. Drones zijn echter niet zomaar inpasbaar. Zo heeft de marine behoefte aan een heel ander soort breedhoekcamera met een veel hogere resolutie, aangezien je op zee over een

brede horizon en in de verte wilt kunnen kijken. Er zijn substantiële aanpassingen nodig om civiele technologie te laten voldoen aan alle militaire functie-eisen.

Een technologie kan alleen militaire toepassingen vinden door inpassing in de militaire operatie. Pas na het maken van deze koppeling is het mogelijk om het civiele aanbod goed te beoordelen en eventueel aan te boren. De kunst is om vanuit een militaire behoefte te kijken welke technologische oplossingen er uit het civiele domein beschikbaar zijn. Momenteel bestaat er een risico tot het kopen van ‘gadgets van de plank’, in plaats van het investeren in langetermijn-kennisontwikkeling die nodig is voor een goede inpassing van nieuwe technologie in militaire systemen.

De verwachtingen van nieuwe ontwikkelingen zijn vaak hoog, maar het duurt lang om een echte innovatie te ontwikkelen die in operaties kan worden ingezet. Startups en het mkb kunnen niet zonder meer die capaciteit bieden. Een eenzijdige focus op deze partijen leidt er vaak toe dat het ‘gadgets’ blijven, hebbedingetjes met weinig substantiële koppeling met de operationele behoefte. Ondanks het toegenomen belang van civiele technologie, blijft er behoefte bestaan aan doelgerichte investeringen in militaire R&D om aan de kennisbehoeften van de Nederlandse marine te kunnen voldoen. Deze koppeling en beoordeling van civiele techniek op inpasbaarheid vergen capaciteit en expertise bij de marine. Het is niet vanzelfsprekend dat de marine de benodigde expertise heeft of kan hebben. Zo is er binnen de marine momenteel discussie over hoeveel kennis er binnenshuis zou moeten zijn rondom nieuwe sleuteltechnologieën als kunstmatige intelligentie.

De vraag is of de marine dit zelfstandig kan oppakken, zonder de hulp en kennis van de partners uit de gouden driehoek. De vertrouwde ketenpartners, zoals MARIN en TNO, spreken dan ook van een ander model, waarin civiel-militaire integratie met name in de keten plaatsvindt terwijl (het belang van) de klassieke gouden driehoek overeind blijft. Gefragmenteerd hebben mkb’ers en startups weinig toegevoegde waarde voor defensie. (Middel)grote organisaties kunnen als kern van een cluster acteren, waarbij mkb en opkomende bedrijven aansluiten in een schil van hoogwaardige toeleveranciers. Het idee is dat MARIN en TNO goed gepositioneerd zijn om deze rol op te pakken, aangezien zij al sinds jaar en dag erg actief zijn op zowel civiel en militair terrein. Dit geldt ook voor de Nederlandse scheepsbouwindustrie. Die trend werd versterkt door het gebrek aan marinebouwwerk in de afgelopen jaren, waardoor het werk van de Nederlandse scheepsbouwindustrie steeds verder verschoof naar export, offshore en civiele scheepsbouw (Overgoor et al., 2018). Met behulp van clusters bouwen de partijen uit de gouden driehoek op een breder netwerk, waarin verschillende civiele partijen, civiele kennis en ook universiteiten betrokken zijn. Van een gouden driehoek naar een gouden ecosysteem (Kik, 2018).

De oorspronkelijke partners van de ‘gouden driehoek’ lopen in deze huidige context wel tegen problemen aan. Door de opkomst van cyber, big data en kunstmatige intelligentie is veel kennis nodig vanuit civiele en commerciële partijen. TNO en MARIN hebben met de huidige budgetten niet de capaciteiten om de kennisbasis voor een moderne marine volledig ‘intern’ te kunnen afdekken. Ook is talent aantrekken moeilijk, aangezien deze kennis op veel plekken gewild is. Traditionele partijen moeten actief op zoek naar nieuwe relaties in het kennisecosysteem, bijvoorbeeld door directer aan te haken op kennis die ontwikkeld wordt op universiteiten, of door meer samen te werken met bedrijven uit de civiele sector, van multinational tot startup.

Niet alle partijen staan zonder meer open voor samenwerking met Defensie. Soms hebben ze principiële bezwaren. Een ander probleem is dat betrokkenheid bij een nationaal defensieproject ‘gedoe’ kan opleveren wanneer de Nederlandse overheid zou bepalen dat je door samenwerking met Defensie over vitale kennis beschikt, maar je tegelijkertijd wel je kansen wilt benutten voor internationale samenwerking of verkoop van bedrijfsonderdelen. Daarnaast kenmerken contracten zich nog steeds door lange doorlooptijden en zwaar gejuridiseerde processen met hoge veiligheids- en kwaliteitseisen, terwijl het marktpotentieel vaak minder is dan in de civiele markt.

3.3.2 Internationalisering

Internationalisering is voor het marinebouwcluster geen nieuwe trend. Europese integratie is vooral zichtbaar binnen de industrie. De meeste spelers zijn al lange tijd internationaal actief. Thales NL is onderdeel van een Frans bedrijf. Hun toeleveringsketen is bijkans nog internationaler. Scheepsbouwers zijn de afgelopen decennia getransformeerd van een partij die alles zelf deed tot ‘integrator’. Ze bezitten wellicht een aantal unieke technologieën, maar functioneren vooral als projectmanager, afhankelijk van een internationaal netwerk van specialistische technologische toeleveranciers.

De nieuwe beleidslijn om nationale belangen voorrang te geven bij de vernieuwing van de Nederlandse vloot is gebaseerd op enig realisme. Nederland is niet meer in staat volledig zelfstandig schepen te ontwikkelen. De industrie is zich gaan specialiseren in specifieke niches, waardoor Nederland met name een sterke kennisbasis en marktpositie heeft op het gebied van scheepsautomatisering en radar- en sensortechnologie.

Internationale samenwerking is daarom een van de grote uitdagingen bij de ontwikkeling en bouw van de nieuwe generatie schepen (Hudson, 2018). Zoals beschreven in hoofdstuk 2 kan dit via drie routes: bilateraal, via de NAVO of in Europees verband. We lichten ze hier kort toe.

Bilateraal
Waar de industrie een sterk internationaal karakter heeft, loopt de internationale samenwerking op het gebied van overheidsinvesteringen in onderzoek, innovatie en materieelaanschaf ver achter. Binnen de EU is 90 procent van de R&D-bestedingen en 80 procent van de materieelaanschaf nationaal georganiseerd[7]. Veel landen hebben een unieke vloot met eigen schepen. Industriële en economische belangen wegen hier geregeld zwaarder dan een gemeenschappelijk veiligheidsbelang.

Maar de komende jaren lijkt daar verandering in te komen. De Nederlandse marine gaat in de ontwikkeling van nieuw materieel verstrekkende samenwerking aan met de Belgische, Duitse en Noorse marine. Aanbestedingen zullen naar alle waarschijnlijkheid worden gegund aan Europese consortia, met partijen uit zowel Nederland als andere Europese landen. Het doel is te komen tot werkelijke integratie, zonder een opeenstapeling van nationale eisen. Nederlandse bedrijven moeten, net zoals de Nederlandse marine, met hun buitenlandse evenknieën leren samenwerken (van Baal, 2014).

De samenwerking met de Belgen is momenteel het meest concreet. De landen hebben afgesproken dat beiden gezamenlijk twee typen schepen gaan vervangen. Nederland heeft de ‘lead’ in de vervanging van fregatten en België krijgt de leiding in de vervanging van mijnenvegers. Bij de nieuwe situatie hoort immers dat je elkaar wat moet gunnen in internationale samenwerking.

NAVO
Binnen de NAVO komt internationale samenwerking tot stand via de NATO Science & Technology Organization. In workshops worden nieuwe ontwikkelingen gesignaleerd en gedeeld. Voor Nederland spelen met name TNO en MARIN hierin een rol. In het maritieme domein vinden diverse gezamenlijke onderzoeksprojecten plaats, bijvoorbeeld op het gebied van alternatieve scheepsvormen. Uit een dergelijk initiatief is de bijlboeg voortgekomen, een boeg in de vorm van een bijl, die zich kenmerkt door een geheel verticale steven en een relatief hoog en smal voorschip. Recent zijn proeven gedaan om te achterhalen in hoeverre de bijlboeg relevant is voor nieuwe fregatten voor de Nederlandse marine. Uit het initiatief kwam een reeks van projecten met NAVO-partners voort, onder andere met de

[7] Bron: EU fact sheet

U.S. Coast Guard. Ook MARIN werkt samen in NAVO-verband. Uit een van deze projecten is bijvoorbeeld de vorm van de huidige generatie patrouilleschepen ontstaan.

Bij de NAVO-samenwerkingsverbanden is het lastiger om tot soortgelijke afspraken te komen als bij bilaterale samenwerking, waar verschillende partijen elkaar iets kunnen gunnen. Vaak blijven de NAVO-samenwerkingsverbanden steken op pre-competitieve samenwerking, omdat meewerkende instituten vanwege diverse nationale belangen niet altijd het achterste van hun tong laten zien.

Europees verband

De nieuwe impuls vanuit de Europese Commissie voor samenwerking rondom defensie en veiligheid biedt kansen. Zowel TNO, MARIN als de Nederlandse scheepsbouwers zoals Damen en RH Marine zijn zich druk aan het voorbereiden op een nieuw EU-budget voor defensieonderzoek. Voor deze partijen is nog onduidelijk welke onderwerpen op de agenda komen en in hoeverre dit aansluit op de kennis en kunde van Nederlandse partijen. Vooralsnog is samenwerking via de EU kansrijk. Zo heeft Damen binnen Horizon 2020 een zeer hoge succesratio (56 procent, ten opzichte van 16 procent voor Nederland gemiddeld). Dat is grotendeels te danken aan de deelname in Euroyards, een consortium van grote Europese scheepswerven waarin scheepsbouwers en andere commerciële partijen hun kennis combineren en met elkaar afstemmen.

Uit de eerste signalen blijkt dat marine-onderzoek een belangrijke tak kan gaan vormen binnen. In 2017 lanceerde de Europese Commissie het *Preparatory Action on Defence Research* (PADR): een driejarig programma voor in totaal 90 miljoen euro. Dit vormt een eerste stap richting een Europees defensieonderzoeksprogramma voor de periode 2021-2027, en dient vooral om ervaring op te doen. Het eerste gefinancierde project binnen PADR is Ocean2020, dat 35 miljoen euro ontving voor onderzoek naar *maritime surveillance*. Het doel van het onderzoek is om drones en onbemande onderzeeërs beter te integreren in operaties van de marinevloot, bijvoorbeeld als kleine flexibel inzetbare *add-ons* van een meer conventioneel fregat. Bij dit onderzoek zijn onderzoeksinstellingen uit 15 lidstaten betrokken, waaronder ook TNO. Hiermee staat Ocean2020 symbool voor de ontwikkelingen binnen het maritieme domein, die ondersteuning moeten bieden bij de nieuwe defensie- en veiligheidsuitdagingen zoals *maritime surveillance* in de digitale samenleving.

Grenzen aan internationalisering

Ondanks dat er grote stappen worden gezet, blijft internationalisering in het maritieme domein lastig. Dit heeft verschillende oorzaken. Ten eerste zorgt de verslechterde veiligheidssituatie ook binnen het maritieme domein voor druk op het

delen van kennis. Een terugkerend discussiepunt is of bepaalde kennis wel in handen van buitenlandse mogendheden mag komen, omdat dit nationale belangen en veiligheid kan schaden. Zo geven gesprekspartners aan dat samenwerken met Rusland vijf jaar geleden een stuk eenvoudiger was dan nu. Ook de opkomst van China en zijn assertieve internationaliseringsstrategie wordt gevoeld. Veel Nederlandse partijen willen in principe graag met Chinese partijen of onderzoekers samenwerken, maar zijn zich steeds meer bewust van het feit dat de Chinese overheid meekijkt. De partijen zoeken naar vormen om hiermee om te gaan.

Ten tweede staan onderliggende economische belangen verdere internationalisering in de weg. Met name grote Europese landen zullen niet snel militaire technologie in of met het buitenland ontwikkelen. Ook al bestaan er op papier geen staatsbedrijven meer, in de praktijk is industriepolitiek en het koesteren van nationale kampioenen nooit verdwenen.

Ten slotte brengen concrete beslissingen rondom kennisdeling lastige dilemma's aan de oppervlakte. Het verdelen van taken levert wellicht efficiëntie op, maar het is tegelijkertijd de vraag welke kennis onmisbaar is om zelf over te beschikken, om te voorkomen dat je op sommige vlakken afhankelijk wordt van een ander land.

3.4 Conclusie

Aan de hand van deze casestudy van kennisontwikkeling in het maritieme domein beschreven we wat de gevolgen van de veranderende veiligheidssituatie zijn voor kennis en innovatie binnen het Nederlandse marinebouwcluster. We beschreven de ontwikkelingen binnen het marinebouwcluster aan de hand van twee trends: het toenemende belang van civiele kennis, en internationalisering. Het toenemende belang van civiele kennis is met name zichtbaar in het nieuwe cyberdomein en rondom sleuteltechnologieën zoals automatisering en robotica. Internationale samenwerking speelt vooral bij de aanstaande vernieuwing van de Nederlandse vloot een prominente rol.

De casestudy laat zien dat internationalisering en civiel-militaire integratie binnen het marinebouwcluster geen nieuwe trends zijn. De industrie is al lange tijd internationaal actief, en geopolitieke spanningen zijn van alle tijden. Ook zijn civiele en militaire kennis bij de meeste hoofdrolspelers gecombineerd binnen één organisatie. Bij de traditionele ketenpartners in de 'gouden driehoek' zijn er dan ook al praktijken ontwikkeld om adequaat te kunnen omgaan met de grenzen tussen militair en civiel., Denk bijvoorbeeld aan geheimhouding, afsluiten van laboratoria en testfaciliteiten of screenen van mensen.

Toch krijgt de samenwerking binnen de nationaal georganiseerde ‘gouden driehoek’ een ander karakter dan vroeger. Zo zijn er meer betrokken partijen en opener verbindingen naar civiele kennisecosystemen. Betrokkenen duiden dit ook wel aan als de overgang van een gouden driehoek naar een gouden ecosysteem. De veranderende samenwerking brengt een aantal nieuwe uitdagingen mee die betrekking hebben op zowel de civiel-militaire integratie als de internationale verhoudingen.

Zo is het een uitdaging om aansluiting vinden op nieuwe civiele kennis, bijvoorbeeld op het gebied van robotica, automatisering en kunstmatige intelligentie. Organisaties hebben niet altijd de capaciteit, komen moeilijk aan goed personeel, of ondervinden moeite bij het aangaan van nieuwe samenwerkingen met de bedrijven of universiteiten waar deze kennis zit. Militaire toepassingen van technologie stellen hoge eisen aan betrouwbaarheid en robuustheid onder extreme omstandigheden. Hierdoor is het vaak complex en kostbaar om civiele innovaties te laten voldoen aan militaire specificaties, zodat ze zijn in te passen in militaire systemen. Partijen die met name civiel actief zijn, hebben andere aanbestedingsbehoeften, andere functie-eisen en kwaliteitsnormen en andere toeleveringsnetwerken. Dit maakt samenwerken met de traditionele gouden driehoek niet eenvoudig.

Daarnaast geldt dat internationale samenwerking nog steeds op veel barrières stuit. Zo is internationale samenwerking in EU- of NAVO-verband voorbij het pre-competitieve niveau vaak lastig. Afwegingen worden lang niet altijd gemaakt op basis van veiligheidsoverwegingen. Economische en industriële belangen spelen een belangrijke rol. Bij verregaande samenwerking, zoals bijvoorbeeld met België of Noorwegen, is altijd de vraag in hoeverre Nederland afhankelijk mag zijn van de kennisontwikkeling en de innovaties van bondgenoten. Ook is aansluiting op de operatie een aandachtspunt. Kun je iets volledig benutten en inzetten, wanneer je niet exact weet hoe het werkt? Ten slotte geldt ook voor het maritieme domein dat nieuwe internationale spanningen leiden tot nieuwe afwegingen wat betreft de partners met wie je wel of niet wil samenwerken, en onder welke voorwaarden.

4 Nieuwe uitdagingen voor de publieke kennisinfrastructuur

In de vorige hoofdstukken lieten we zien dat er sprake is van een nieuwe digitale wapenwedloop, die op het gebied van kennisontwikkeling anders is dan de wapenwedlopen uit het verleden. Overheden kunnen niet meer uitsluitend terugvallen op nationaal georganiseerde militaire kennisecosystemen, maar moeten in toenemende mate een beroep doen op internationaal vervlochten en civiele kennisecosystemen.

In dit hoofdstuk richten we ons op de vraag wat deze ontwikkeling betekent voor de publieke kennisinfrastructuur die zich geconfronteerd ziet met die situatie. We identificeren drie belangrijke vraagstukken waar publieke kennisinstellingen nu voor staan:

- Hoe verhouden kennisinstellingen zich tot kennisontwikkeling met expliciet militaire doeleinden?
- Hoe kunnen kennisinstellingen omgaan met *dual-use* in het digitale tijdperk?
- Welke verantwoordelijkheid hebben kennisinstellingen in het waarborgen van defensie- en veiligheidsbelangen?

4.1 Kennisontwikkeling met expliciet militaire doeleinden

Digitalisering leidt tot tal van nieuwe militaire toepassingen. Sommige partijen spelen op dit gebied vanzelfsprekend een rol in de kennisontwikkeling. In hoofdstuk 2 lieten we zien dat in Nederland historisch gezien TNO hiervoor de aangewezen partij is. Ook vandaag de dag is TNO Defensie en Veiligheid nog een grote tak binnen de organisatie, en vormen zij de aangewezen partij wanneer het gaat om het nadenken over militaire toepassingen rondom *virtual reality, augmented reality*, robotica en kunstmatige intelligentie.

TNO krijgt dan ook veel nieuwe geldstromen ter beschikking voor onderzoek en innovatie op het gebied van defensie en veiligheid, vanuit zowel Nederland als Europa. Dit biedt een kans om fondsen te werven. Zie bijvoorbeeld het succes van TNO bij Europees security-onderzoek, waar TNO na het Duitse *Fraunhofer* en het Zweedse *Swedish Defense Research Agency* met ruim 33 miljoen euro de twee-na-grootste ontvanger is van deze Europese onderzoeksgelden (Tokmetzis &

Goslinga, 2017). Ook in het aanstaande Europese Defensiefonds zal TNO proberen aanspraak te maken op de nieuwe fondsen.

Naast TNO kunnen ook andere publieke kennisorganisaties met een voorheen (deels) militaire taakstelling een belangrijke rol spelen in de Nederlandse kennisontwikkeling voor defensie en veiligheid. Denk aan NLR en MARIN, die respectievelijk expertise hebben op het vlak van de luchtmacht en de marine. Niet minder belangrijk zijn Clingendael en de NLDA: de twee publieke kennisorganisaties die niet direct een technologische expertise hebben, maar wel een belangrijke functie vervullen in het in stand houden van een kennisbasis met betrekking tot respectievelijk internationale betrekkingen en militaire geschiedenis en operaties.

Gezien de nieuwe veiligheidscontext is het wel de vraag in hoeverre deze traditionele partijen in staat zullen zijn om volledig te voldoen aan de kennisbehoeften van de Nederlandse overheid. Meer dan voorheen doen kennis- en innovatieagenda's op het gebied van defensie en veiligheid een beroep op civiele actoren uit de publieke kennisinfrastructuur, aangezien deze beschikken over *state-of-the-art* kennis over de relevante technologieën.

Zo laten Bos et al. (2017) zien dat verschillende Nederlandse universiteiten over een sterke en soms internationaal toonaangevende kennisbasis beschikken op het gebied van onder andere geautomatiseerde methodes om kwetsbaarheden in software en hardware te detecteren, postquantum cryptografie, *machine learning* op grote datasets, internet en netwerk security met een focus op detectie en bescherming tegen Distributed Denial of Service (DDoS) of Domain Name System (DNS) aanvallen.

Binnen het bestel aan NWO- en KNAW-instituten is er geen instituut dat zich specifiek richt op thema's rondom defensie en veiligheid. Toch wordt ook hier wel degelijk kennis ontwikkeld die, net als bij de voormalige FOM-instituten rondom nucleaire fysica, van strategisch belang kan zijn vanuit een defensie- en veiligheidsperspectief. Met name het NWO-instituut Centrum Wiskunde en Informatie (CWI) kent veel raakvlakken - zie bijvoorbeeld de titel van hun strategisch plan voor de jaren 2019-2024: *CWI and its role in the digitizing society*.

Op verschillende plekken in de wereld zien we een intensivering van de samenwerking tussen universiteiten en de defensie-industrie. Zo heeft de Australische overheid in 2016 een investering van 2,4 miljard euro in de wapenindustrie aangekondigd. De hoop is dat Australië een van 's werelds top 10 wapenexporteurs zal worden. De overheid heeft zich tot universiteiten gewend om te helpen bij het bereiken van deze doelen.

Het land heeft afgestudeerden nodig met de juiste vaardigheden om de militaire industrie te ondersteunen, evenals academisch onderzoek dat bijdraagt aan de ontwikkeling van militaire technologieën. Universiteiten geven hier gehoor aan: 32 Australische universiteiten hebben zich aangesloten bij het Defence Science Partnership Programme van het Australische ministerie van defensie (Australian Government Department of Defense, 2014).

De ontwikkelingen zorgen ook voor nieuwe publiek-private samenwerking. In 2017 kondigde de universiteit van Melbourne een onderzoekssamenwerking aan met Lockheed Martin - 's werelds grootste wapenfabrikant. Ze richtten een gezamenlijk onderzoekscentrum op dat grenst aan de campus van de universiteit. Dit is het eerste onderzoekscentrum van Lockheed Martin buiten de VS. In 2018 tekende de universiteit van Melbourne nog een soortgelijke overeenkomst – dit keer met de Britse wapenfabrikant BAE Systems (Edney-Browne & Ruff, 2018).

Ook in Nederland komt er meer samenwerking tussen universiteiten en de defensie-industrie. Zo liepen er in 2014 meer dan tien samenwerkingsprojecten tussen de TU Twente en Thales NL, zoals het project DAISY waarin wordt gewerkt aan een radarmodule met een geavanceerde sensortechnologie. In het *Virtual Reality lab T-Xchange* wordt onder meer *serious gaming* gebruikt voor het nabootsen van crisissituaties of het testen van nieuwe projecten en diensten (Krijnsen, 2014). Bij de TU Eindhoven wordt samengewerkt aan de ontwikkeling van pantserglas. Traditioneel is TU Delft ook regelmatig betrokken bij onderzoek met of voor Defensie. Het bekendste voorbeeld is Neder Radarland, een samenwerking tussen de Nederlandse overheid, Thales, TNO en de TU Delft, waarbinnen zij al sinds 2002 gezamenlijk werken aan de ontwikkeling van radarcapaciteiten van de Nederlandse Marine. Recente voorbeelden zijn bijdrages van de TU Delft aan de ontwikkeling van de F-35 (ook bekend als de ‘Joint Strike Fighter’), en de ontwikkeling van een eerste satelliet voor de Koninklijke Luchtmacht.

Weerstand bij universiteiten

Tegelijkertijd zien we veel bezorgdheid over universitair onderzoek dat gebruikt wordt voor militaire doeleinden. Zoals we in hoofdstuk 2 lieten zien, zijn zulke zorgen niet nieuw. Onderzoekers en universiteiten worstelen al lange tijd met de vraag of onderzoek voor defensie en veiligheid past binnen de (publieke) missie van de universiteit, of dat universiteiten enkel een civiele missie hebben. Zo zou onderzoek voor defensie de integriteit van onderzoek(ers) aantasten. Exemplarisch voor dit dilemma is de controverse rondom de atoombom, waarbij Oppenheimer vlak na het bombardement op Hiroshima de woorden uitsprak: ‘*Now I am become Death, destroyer of worlds*’ (Temperton, 2017). In het verleden zette ook de Vietnamoorlog dit debat op scherp, toen grootschalige inzet van Agent Orange en

Napalm de destructieve gevolgen van wetenschappelijke vooruitgang blootlegden. Een recent voorbeeld van de spanning tussen onderzoek voor defensie en veiligheidsdoeleinden enerzijds en wetenschappelijke integriteit anderzijds komt eveneens uit de VS, waar de *American Psychological Association* stevige kritiek uitte over het aandeel van psychologen in *'enhanced interrogation methodes'* – oftewel martelpraktijken – in de oorlog tegen het terrorisme (Downs & Sharpless, 2015).

De afgelopen twee jaar zagen we veel voorbeelden van individuele onderzoekers die stelling namen tegen defensie- en veiligheidsgerelateerd onderzoek. Zo kwamen bezorgde wetenschappers in 2018 met een petitie tegen het voorstel van de Europese Commissie voor Europees defensieonderzoek (Researchers for Peace, 2017). Veel aandacht gaat uit naar autonome wapensystemen. In 2016 riepen wetenschappers van over de hele wereld op tot een boycot van onderzoek op het gebied van zogeheten *LAWS: Lethal Autonomous Weapon Systems* (Sample, 2017). Ook zette een wereldwijd netwerk van onderzoekers de Zuid-Koreaanse kennisinstelling *Korea Advanced Institute of Science and Technology* onder druk om niet meer samen te werken met wapenfabrikant Hanwha Systems, die samen met de universiteit een leger van robots wilde ontwikkelen (Shalal, 2018).

Sommige universiteiten nemen als geheel stelling tegen defensieonderzoek. Zo heeft Kyoto University aangekondigd geen geld meer te accepteren van het Japanse ministerie van Defensie, nadat de Japanse overheid aankondigde het budget voor defensieonderzoek te verachttienvoudigen (Johnston, 2018). In Duitsland hebben tot nu toe 18 universiteiten een *civil clause* ondertekend, die onderschrijft dat de universiteit alleen een civiele missie heeft en daarom alleen civiel onderzoek doet (Schulze, 2014). Ook Nederland kent een traditie van universiteiten die hun civiele missie benadrukken. Een recente uitspraak van de voormalige rector van de Universiteit Utrecht, Bert van der Zwaan, past in die traditie. Aan de Volkskrant liet hij weten dat zijn universiteit geen geld accepteert van de wapenindustrie en ook geen onderzoek wil doen dat de wapenindustrie mogelijk kan gebruiken (Mudde, 2018). Zullen Nederlandse universiteiten het Duitse en Japanse voorbeeld volgen?

4.2 *Dual-use* in de digitale samenleving

De bovenstaande paragraaf ging over kennis die met een expliciet militair doel is ontwikkeld. Maar in het hoofdstuk 2 beschreven we al dat digitale kennis die oorspronkelijk is ontwikkeld met een civiel doel onbedoeld ook veel militaire toepassingen kan hebben. Dit maakt het moeilijk om vooraf vast te stellen of de

ontwikkelde kennis zal raken aan defensie- en veiligheidsbelangen. Er zijn tal van voorbeelden van kennis die werd ontwikkeld met ogenschijnlijk civiele doeleinden, om vervolgens met andere intenties te worden toegepast. Een bekend recent voorbeeld is het schandaal rondom het bedrijf Cambridge Analytica. Verschillende academici van de University of Cambridge, met name van de afdeling Psychologie en het Psychometrics Centre, hielpen Cambridge Analytica bij het ontwikkelen van haar online psychometrische technieken (Laterza, 2018). Die technieken werden vervolgens ingezet om doelbewust democratische verkiezingen te beïnvloeden door gericht nepnieuws te verspreiden.

In het gangbare afwegingskader voor deze dilemma's wordt gekeken naar dual-use: heeft een onderzoeksresultaat, een nieuwe technologie of een innovatie naast een wetenschappelijke of civiele betekenis ook een militaire betekenis? En meer specifiek: kan er schade mee worden toegebracht? Wanneer deze vraag positief wordt beantwoord, en het betreffende onderzoek is bestempeld als dual-use, kan dit leiden tot verscherpte procedures. Bijvoorbeeld als het gaat om wie er toegang heeft tot een lab of met welke onderzoekers uit welke landen mag worden samengewerkt. Wanneer het onderzoek tot een concreet product leidt, wordt vervolgens de vraag gesteld of er een exportvergunning nodig is[8].

Dual-use richt zich traditioneel op biologisch, chemisch of nucleair onderzoek en innovatie. Met de opkomst van het cyberdomein en het toenemende belang van civiele kennisontwikkeling rondom sleuteltechnologieën (zoals kunstmatige intelligentie en robotica) is er tegenwoordig veel meer onderzoek met een dual-use karakter. Bij veel van die kennis is het lastig om een duidelijk onderscheid te maken tussen civiele en militaire kennisontwikkeling. Steeds vaker komt dit onderscheid pas op een zeer hoog *technology readiness level* – dicht op de uiteindelijke toepassing. Het is daarom de vraag of dual-use nog wel als onderscheidend kenmerk gebruikt kan worden. Veel onderzoek bevat mogelijk aspecten die relevant zijn voor defensie en veiligheid. Het wordt steeds moeilijker om vooraf te bepalen welke specifieke toepassingen van wetenschap en technologie potentieel problematisch zijn. Te midden van die complexiteit is het gebruik van dual-use als onderscheidende factor wellicht niet langer toereikend om op een weloverwogen manier de belangen van wetenschap en veiligheid tegen elkaar te kunnen afwegen.

De wens van de voormalig rector magnificus van de UU, Bert van der Zwaan, om geen onderzoek te doen dat de wapenindustrie *zou kunnen* helpen, lijkt steeds

---

8 Voor Nederland is de export van dual-use goederen op Europees niveau geregeld. De Europese Commissie heeft een lijst opgesteld van goederen die alleen met een vergunning kunnen worden geëxporteerd, en die jaarlijks wordt herzien. Ondanks dat dit vooralsnog een vrij conventionele lijst betreft, die vooral betrekking heeft op biologische, chemische en nucleaire goederen, is dit al een lijvig document. De Europese Commissie bekijkt momenteel of het tot een nieuwe definitie van dual-use kan komen, waarin ook meer aandacht is voor mensenrechten en cyber. Gezien de nu al flinke omvang zal een nieuwe definitie hoogstwaarschijnlijk leiden tot een nog langere lijst van nieuwe technologieën en vakgebieden.

lastiger. Want kan kennis voor de ontwikkeling van een zelfrijdende auto niet ook dienen om autonome wapensystemen te verbeteren? En wat schaar je in het cybertijdperk precies onder wapens? Is desinformatie ook een wapen? Dit alles roept de vraag op hoe naïef je nog mag zijn als onderzoeker of kennisinstelling.

Dual-use en internationalisering

De nieuwe internationale spanningen maken deze afwegingen niet makkelijker. Onderzoek met civiele doeleinden is al eeuwenlang een mondiale activiteit, waarbij onderzoekers internationaal samenwerken om hun kennis te verbreden en te verdiepen. *Open science* is momenteel een belangrijke waarde binnen de wetenschap. De Europese Commissie promoot dit discours onder het motto: '*open science, open innovation, open to the world'*.

Openheid is belangrijk voor de vooruitgang en welvaart van moderne samenlevingen. Maar hoe verhoudt het zich tot de toenemende internationale spanningen en de ontluikende wapenwedloop rondom tal van nieuwe technologieën? Dit laatste botst met de waarde van open en internationale wetenschap, aangezien het de vertrouwensrelaties afbreekt die wetenschappers over de hele wereld met elkaar verbinden. Het delen van gegevens, technieken en publicaties vormde de basis van vreedzame samenwerking, zelfs tussen onderzoekers uit landen die met elkaar in conflict waren. Dit soort samenwerking lijkt steeds complexer: 'als onderzoekers zich af moeten vragen of hun bijdragen de ontwikkeling van een wapen zullen voeden, kunnen ze – begrijpelijk – hun ideeën voor zichzelf houden' (Nature, 2018).

Deze afwegingen winnen aan actualiteit. Vooral de relatie met China leidt momenteel tot spanningen. Zo staken Chinese techgiganten de afgelopen jaren veel geld in Amerikaanse tech-startups: ze besteedden rond de 5,5 miljard dollar in een vijftigtal deals. Het betreft met name ICT-technologie, veelal met mogelijk militaire toepassing, onder andere van startups die vanuit de eigen overheid weinig investeringen kregen (Mozur & Perlez, 2017). Deze ontwikkeling baarde politici zorgen, onder andere in het Pentagon. Onder politieke druk werden Chinese overnames voorkomen. Dankzij interventies en een versoberd Chinees financieel beleid daalden overnames met 87 procent in 2017 (Minaya, 2018). Op verzoek van Duitsland, Frankrijk en Italië maakte de Europese Commissie in 2017 een voorstel om buitenlandse overnames in infrastructuur, hightech en energie in de EU te screenen (de Gruyter, 2018). China zelf investeert strategisch in bepaalde Europese sectoren die corresponderen met hun doelen in beleidsplannen, zoals *Made in China 2025*.

De Chinese inmenging is ook zichtbaar bij kennisinstellingen. Zo laat een onderzoek van het *Australian Strategic Policy Institute* zien hoe het Chinese leger

zijn onderzoekssamenwerking uitbreidt met universiteiten buiten China. Sinds 2007 heeft het leger meer dan 2.500 militaire wetenschappers en ingenieurs gefinancierd om in het buitenland onderzoek te doen. Ook ontwikkelde het Chinese leger relaties met onderzoekers en instellingen over de hele wereld. De Chinese onderzoekers zijn meestal verbonden aan de PLA *National University of Defense & Technology* of *the Army Engineering University*, maar geven vaak valse civiele instituties op als moederuniversiteit, om zo minder op te vallen (Joske, 2018). Een studie van het Leiden Asia Centre stelt dat wetenschap in China is afgestemd op de veiligheidsbehoeften en de strategische visie van de staat, terwijl aan de Europese kant van de samenwerking een duidelijke strategie ontbreekt en behoefte is aan een betere toetsing van de verschillende risico's ten opzichte van de opbrengsten (Pieke et al., 2018).

In Nederland liet het ministerie van Buitenlandse Zaken een checklist opstellen voor samenwerking met Chinese academische en kennisinstellingen. Hiermee wil het ministerie bespreekbaar maken hoe Nederlandse academische en kennisinstellingen die samenwerken met China hun verschillende belangen kunnen afwegen, hoe er meer bewustzijn kan worden gecreëerd voor mogelijke risico's, en wat de mogelijkheden zijn om die risico's in te perken (Bekkers et al., 2018).

Amerikaanse universiteiten gaan al een stap verder, en volgen bijvoorbeeld de eigen regering in het boycotten van Chinese technologiebedrijven zoals Huawei. Ook de Britse Oxford University heeft een kant gekozen, en zette de samenwerking met Huawei per direct stop, inclusief twee lopende onderzoeksprojecten ter waarde van bijna 1 miljoen euro (Davies, 2019).

4.3 Waarborgen van defensie- en veiligheidsbelangen bij kennisontwikkeling met civiele doeleinden

Een laatste punt van aandacht is kennis die ontwikkeld wordt voor civiele doeleinden en ook civiel wordt toegepast, maar onbedoeld alsnog leidt tot nieuwe kwetsbaarheden op het gebied van defensie en veiligheid. Zo leidt digitalisering tot kwetsbaarheden in de civiele infrastructuur, bijvoorbeeld bij banken, energiebedrijven en de zorg. Als gevolg worden kennisinstellingen en bedrijven die zich primair op de civiele markt richten, nu steeds vaker beschouwd vanuit een defensie- en veiligheidsperspectief. De komende jaren staan in het teken van tal van digitaliseringsprocessen die de fysieke wereld en het cyberdomein steeds inniger met elkaar verbinden. Denk aan de uitrol van het 5G-netwerk of de introductie van de zelfrijdende auto. Kennisinstellingen zullen hierin een belangrijke rol spelen.

Van kennisinstellingen wordt steeds vaker verwacht dat defensie- en veiligheidsaspecten meer zijn dan een zorg voor later. De nieuwe kwetsbaarheden van de digitale samenleving onderstrepen de noodzaak om meer structurele oplossingen voor deze problemen te ontwikkelen, waarbij defensie- en veiligheidsaspecten een standaard onderdeel moeten worden van de beoordeling van onderzoeksprocessen – van voorstel tot evaluatie. Dit vraagt bijvoorbeeld om s*ecurity-by-design* – het vooraf inbouwen van een aantal preventieve maatregelen in het publieke belang van defensie en veiligheid. Onder *security-by-design* vallen uiteenlopende initiatieven zoals beperking van de functionaliteit van *internet of things*-apparatuur, het herontwerp van delen van de ICT-infrastructuur, of het gebruik van decentrale of gedistribueerde dataopslag.

5 Conclusies

De geopolitieke verhoudingen in de wereld zijn aan het verschuiven, zo hebben we in dit rapport gezien, vooral door de opkomst van China als nieuwe mondiale speler. In deze nieuwe geopolitieke werkelijkheid staan kennis en innovatie als strategisch middel voor militaire macht weer bovenaan de politieke agenda. Wereldwijd worden nieuwe kennis- en innovatieagenda's geformuleerd om op strategische kennisgebieden een voorsprong te ontwikkelen of te behouden. Met name digitalisering wordt gezien als een bepalende technologische ontwikkeling.

Ook in het verleden werden technologische superioriteit en voorsprong in kennis als cruciaal gezien om de tegenstander voor te blijven. Berucht is de wapenwedloop tijdens en na de Tweede Wereldoorlog. Diverse overheden investeerden in onderzoekscentra en laboratoria voor defensieonderzoek en de ontwikkeling van een eigen defensie-industrie. In dit rapport lieten we zien wat de verschillen zijn tussen deze historische en de huidige wapenwedloop. We stellen dat de huidige context op twee facetten een andere dynamiek kent in vergelijking met de wapenwedloop tijdens de Koude Oorlog:

- **Het vervagen van het onderscheid tussen kennisontwikkeling voor civiele en militaire doelen**. Met name digitalisering leidt ertoe dat het onderscheid tussen kennisontwikkeling voor civiele en militaire doelen steeds lastiger te maken is. Bovendien creëren civiele toepassingen van digitale technologieën allerlei nieuwe kwetsbaarheden.
- **Het internationaliseren van kennisontwikkeling en innovatie, in het bijzonder die gericht op defensie en veiligheid**. Kennisontwikkeling vindt steeds meer plaats in internationale samenwerking. Dat geldt ook voor kennisontwikkeling voor defensie en veiligheid.

In dit rapport hebben we gekeken naar de gevolgen van deze trends voor de publieke kennisinfrastructuur, bestaande uit universiteiten en hogescholen, wetenschappelijke instituten en publieke kennisorganisaties. We maken onderscheid tussen de TO2-instellingen TNO, MARIN en NLR - die van oudsher een belangrijke rol spelen in militaire kennisecosystemen - en de overige publieke kennisinstellingen die niet of nauwelijks onderdeel hiervan waren.

Hiermee agenderen we de belangrijkste opgaven en dilemma's voor de komende jaren, en identificeren we op welk niveau, van individuele onderzoeker tot internationale verbanden, deze het best kunnen worden geadresseerd.

Gevolgen voor de van oorsprong militair georiënteerde kennisinstellingen
In dit rapport beschreven we de gevolgen voor de kennisinstellingen die zich van oudsher, als onderdeel van hun activiteiten, op militaire kennisontwikkeling richten, en voor instellingen die onderzoek verrichten ten behoeve van de marine - zoals TNO en MARIN. De casestudy over het maritieme domein laat zien dat de hechte samenwerking die in de loop der tijd ontstond tussen overheid, publieke kennisinstellingen en bedrijfsleven (soms aangeduid als ‘de gouden driehoek’), belangrijk blijft voor het borgen van een strategische kennisbasis. Wel dwingen de genoemde trends deze partijen tot meer verbindingen met civiele kennisecosystemen, omdat militaire technologieontwikkeling steeds meer voortbouwt op civiele technologie. Zo kunnen civiele drones relatief eenvoudig worden doorontwikkeld tot robotwapens.

Ook werken de publieke kennisorganisaties steeds meer over de grens, vaak in internationale samenwerkingsverbanden. Dat versterkt hun kennisbasis en biedt mogelijkheden om de positie van Nederland in de wereld te versterken (Diercks et al., 2018). De internationalisering vraagt ook om meer taakverdeling en specialisatie. Dat roept de vraag op in hoeverre een kennisinstelling de benodigde kennis zelf in huis moet hebben en in welke mate de instelling afhankelijk kan zijn van de kennisbasis van nieuwe, soms buitenlandse, partners.

Deze ontwikkelingen leiden ertoe dat de gouden driehoek-gedachte plaatsmaakt voor een ‘gouden ecosysteem’-gedachte, waarin de verschillende publieke kennisorganisaties een andere rol gaan spelen in het vervullen van de kennisbehoefte van de Nederlandse krijgsmacht. Ze zijn niet meer het huislaboratorium, maar een strategische kennispartner met een publieke taak.

Gevolgen voor de van oorsprong civiel georiënteerde kennisinstellingen
De gevolgen van de genoemde trends zijn ingrijpender voor de partijen die voorheen vooral onderdeel waren van civiele kennisecosystemen.

- Een eerste gevolg is dat voor de nieuwe kennis- en innovatieagenda’s op het gebied van defensie en veiligheid vaker een beroep wordt gedaan op civiel georiënteerde kennisinstellingen, aangezien deze beschikken over *state-of-the-art* kennis over kunstmatige intelligentie, robotica en cybersecurity.
- Een tweede gevolg is dat het voor onderzoekers steeds moeilijker wordt om vooraf te bepalen welke specifieke ontwikkelingen van kennis en technologie potentieel militaire betekenis hebben of veiligheidsrisico’s met zich meebrengen. Ook hier speelt digitale technologie een belangrijke rol vanwege het generieke karakter: onderzoek en innovatie in de civiele sfeer zetten geregeld onbedoeld de deur open naar de ontwikkeling van toepassingen voor militaire doeleinden.

- Een derde gevolg is dat civiele kennis- en technologieontwikkeling die vormgeeft aan de digitale samenleving, nieuwe zwakke plekken introduceert met consequenties voor defensie en veiligheid; vooral vanwege het feit dat digitale apparaten allemaal in netwerken met elkaar verbonden zijn.

De directe en indirecte betrokkenheid van de publieke kennisinfrastructuur bij kennisontwikkeling die raakt aan defensie en veiligheid moet door dit alles opnieuw doordacht en waar nodig anders georganiseerd worden. Omdat de gevolgen voor de civiele georiënteerde kennisinstellingen nieuwer en ingrijpender zijn dan voor die instellingen waar militaire kennisontwikkeling altijd al onderdeel was van het takenpakket, richten we ons in dit slothoofdstuk op het (voorheen) civiel georiënteerde deel van de publieke kennisinfrastructuur.

Dit rapport laat zien hoe kennisinstellingen en hun onderzoekers die zich voorheen een uitsluitend civiele missie toedichtten, geconfronteerd worden met de keuze of en onder welke voorwaarden zij willen bijdragen aan onderzoek voor defensiedoeleinden. Op verschillende plekken in de wereld vindt een intensivering plaats van de samenwerking tussen universiteiten en de defensie-industrie. Tegelijkertijd observeren we dat er veel bezorgdheid is over universitair onderzoek dat voor militaire doeleinden wordt gebruikt. Zo ondertekenden 18 universiteiten in Duitsland een *civil clause*, die onderschrijft dat de universiteit uitsluitend een civiele missie heeft, en daarom alleen civiel onderzoek wil doen. In onze historische analyse lieten we zien dat onderzoek voor militaire doeleinden door universiteiten in Nederland historisch gevoelig ligt. Zullen Nederlandse universiteiten het Duitse voorbeeld volgen?

De beweging van Duitse universiteiten is interessant en begrijpelijk vanuit het perspectief van studenten en medewerkers die vrezen voor een militarisering van de universiteit. Tegelijkertijd zijn defensie en veiligheid breed gedragen politieke doelen, en worden ze steeds vaker gedefinieerd in termen van maatschappelijke uitdagingen. Vanuit maatschappelijk perspectief is het dus de vraag in hoeverre het wenselijk is wanneer een (groot) deel van de publieke kennisinfrastructuur bij voorbaat haar handen aftrekt van onderzoek voor militaire doeleinden.

Daar komt bij dat onderzoek voor militaire doeleinden veel breder is dan alleen onderzoek naar offensief inzetbare technologie. Een breed scala aan kennis- en technologieontwikkelingen kan van militaire betekenis zijn. Onze maatschappij heeft behoefte aan een breed palet aan typen kennis, zoals *intelligence* over nieuwe soorten dreigingen, ethische kaders voor autonome wapens, onderzoek naar en duiding van nepnieuws, of een beter begrip van de motieven van Amerika, Rusland of China. Juist hier kunnen inzichten van kennisinstellingen die voorheen met name civiel onderzoek deden, van grote waarde zijn.

Het gaat dus niet altijd om technologie die offensief kan worden ingezet: soms betreft het juist technologie voor uitgesproken defensieve toepassingen. Ook gaat het niet alleen om destructieve toepassingen: de kennis is bijvoorbeeld ook van belang voor ontwikkeling van nieuwe protheses, onderzoek naar posttraumatische stressstoornissen, of historisch onderzoek. En zoals we al lieten zien: niet alleen kennis en technologie met militaire toepassingen vragen om kaders, maar ook kennis en technologie die mogelijk nieuwe kwetsbaarheden in civiele systemen introduceren.

Deze nadruk komt ook terug in de 25 missies die het kabinet in april 2019 vaststelde voor het topsectoren- en innovatiebeleid. Onder het thema Veiligheid zijn onder leiding van het ministerie van Defensie en het ministerie van Justitie & Veiligheid zes missies[9] geformuleerd die moeten bijdragen aan een veiliger samenleving, een weerbaarder Nederland, én het creëren van economische kansen. De missies hebben een brede insteek en stellen dat in het veiligheidsdomein niet alleen nieuwe technische kennis moet worden ontwikkeld, maar dat er ook behoefte is aan sociaal, maatschappelijk, juridisch, gedragswetenschappelijk, organisatorisch, sociaalpsychologisch en (geo)politiek onderzoek. Dit vraagt om expertise die niet per definitie te vinden is binnen de van oorsprong militair georiënteerde kennisinstellingen, zoals TNO, MARIN en NLR. Het bij voorbaat distantiëren van deze agenda's door van oorsprong civiel georiënteerde kennisinstellingen kan juist contraproductief zijn. Zonder deze bredere inzichten is er namelijk een groter risico dat militair onderzoek zich beperkt tot een uitsluitend technologische insteek - met alle potentiële ongewenste maatschappelijke effecten van dien.

Uit onze analyse blijkt daarnaast dat het maar de vraag is of het überhaupt mogelijk is om je als kennisinstelling uitsluitend op civiel onderzoek te oriënteren. Gezien de vervaging van het onderscheid tussen militaire en civiele kennis, is het steeds moeilijker om vooraf vast te stellen of de ontwikkelde kennis zal raken aan defensie- en veiligheidsbelangen. In dit licht bezien is de effectiviteit van een *civil clause* dus beperkt, en is er hoe dan ook meer nodig om de betrokkenheid van de publieke kennisinfrastructuur opnieuw te doordenken en waar nodig anders te organiseren. In de rest van dit hoofdstuk identificeren we achtereenvolgens drie kwesties die bij de publieke kennisinstellingen – en dan gaat het specifiek om universiteiten, hogescholen, TO2-instellingen en Rijkskennisinstellingen – om aandacht vragen.

---

9 De zes missies zijn: Integrale aanpak van georganiseerde criminaliteit; Maritieme hightech voor een veilige zee; Veiligheid in en vanuit de ruimte; Cyberveiligheid; Genetwerkt optreden op land en vanuit de lucht en Samen sneller innoveren voor een adaptieve krijgsmacht.

Die drie kwesties zijn de volgende:

1. *Welke activiteiten hebben mogelijk militaire betekenis?* Welke activiteiten van kennisinstellingen zijn van militaire betekenis of hebben mogelijk consequenties op het gebied van veiligheid en vragen daarom om beleid?
2. *Wie is verantwoordelijk?* Wie moet hier beleid op voeren – wie stelt kaders en wie implementeert? En welke belangen en waarden zijn daarbij in het spel? Wat zijn relevante afwegingen die gemaakt moeten worden als er sprake is van ontwikkeling van kennis en technologie met mogelijk militaire betekenis?
3. *Welke vervolgstappen zijn er nodig?* Welke handelingsopties zijn er en welke voorwaarden of waarborgen kunnen mogelijk worden verlangd?

5.1 Thema's van mogelijk militaire betekenis

Voor civiele kennisinstellingen is het van belang om alert te zijn op zaken en activiteiten die een veiligheidsrisico kunnen introduceren of die van belang kunnen zijn voor militaire doelen. Dat gaat verder dan het wel of niet uitvoeren van specifiek onderzoek of het ontwikkelen van een bepaalde technologie. Onze analyse laat zien dat er meer zaken zijn die raken aan defensie en veiligheid. Wij zien de volgende zes aspecten die vragen om alertheid en beleid:

- *Inhoud van het onderzoek.* Uiteraard vraagt de inhoud van het onderzoek aandacht: heeft dat (mogelijke) militaire betekenis, of kan het leiden tot nieuwe kwetsbaarheden? Wat betekent dit voor het wel of niet participeren in dit onderzoek? Onder welke voorwaarden kan dat wel of niet?
- *Open Science.* Van oudsher kent het wetenschappelijk onderzoek een traditie van open communicatie. Deze traditie heeft de afgelopen tijd een nieuwe impuls gekregen vanuit het beleid gericht op *open science: het inrichten van de wetenschappelijke praktijk op een zodanige manier dat anderen kunnen samenwerken en bijdragen, en waar onderzoeksgegevens, laboratoriumnotities en andere data vrij beschikbaar zijn*[10]. Maar als deze kennis leidt tot militair misbruik, dient *open science* de samenleving niet. Hoe ver moet deze openheid gaan in het licht van veiligheidsbelangen?
- *Fysieke en digitale infrastructuur.* Toegang tot laboratoria, computerfaciliteiten en digitale netwerken was binnen civiel georiënteerde kennisinstellingen tot dusver vaak soepel geregeld. Mogelijk moeten de huidige ontwikkelingen aanleiding geven tot aanscherping van procedures. Als er potentieel gevoelige activiteiten plaatsvinden binnen de instelling, welke voorzorgsmaatregelen

10 Gebaseerd op de definitie zoals gegeven door openscience.nl, *www.openscience.nl/open-science/wat-is-open-science*.

moeten dan worden getroffen? Zijn laboratoria, testfaciliteiten en de digitale infrastructuur voldoende beveiligd?

- *Wervings- en personeelsbeleid.* Mogelijk brengt de werving van onderzoekers of studenten uit niet-bondgenootlanden veiligheidsrisico's mee. Welke mensen kunnen zonder risico toegelaten worden en in welke gevallen is het verstandig om mensen te weren? Welke voorwaarden moeten er gesteld worden en in hoeverre (en door wie) zouden mensen gescreend moeten worden?
- *Bronnen van financiering.* Sommige bronnen van financiering kunnen leiden tot ongewenste afhankelijkheden. Is het acceptabel dat onderzoekers en instellingen geld van het ministerie van Defensie accepteren? Of van overheden en bedrijven met militaire connecties uit andere landen? Wanneer wel/niet; onder welke voorwaarden?
- *Internationaliseringsactiviteiten.* Internationale samenwerking biedt talloze voordelen en kansen, ook wanneer het met niet-bondgenoten is, bijvoorbeeld met betrekking tot financiering van onderzoek of toegang tot talent, data en faciliteiten. Maar samenwerking met buitenlandse partners, het openen van vestigingen in het buitenland en je begeven op internationale markten kan met veiligheidsrisico's gepaard gaan. Welke maatregelen kunnen worden genomen om deze te beperken?

De genoemde aspecten zijn niet volstrekt nieuw. Maar de huidige omstandigheden vragen van de oorspronkelijk civiel georiënteerde kennisinstellingen wel om meer systematische aandacht dan in het verleden. Voorheen waren militaire kennisecosystemen duidelijk afgescheiden van civiele kennisecosystemen, en richtten maatregelen om veiligheidsrisico's in te perken zich voornamelijk op biologisch, chemisch, radioactief en nucleair onderzoek, de zogeheten BCRN.

5.2 Verdeling van verantwoordelijkheden

De verantwoordelijkheid voor het omgaan met de zes hierboven genoemde aspecten is verdeeld over drie niveaus: dat van de politiek, van de instelling en van de individuele onderzoeker. Van onderzoekers mag worden verwacht niet naïef te zijn, en het is voor hen belangrijk dat zij hun kennis en zorgen inbrengen in het publieke debat. Kennisinstellingen kunnen zelf een voorzet geven voor hoe bepaalde afwegingskaders en procedures geïmplementeerd zouden kunnen worden. Maar de veiligheidsbelangen reiken verder dan de individuele onderzoeker of kennisinstellingen – het zijn nationale belangen. Het is niet wenselijk dat individuele onderzoekers eigenstandig afwegingen maken of kennisinstellingen eigen, onderling verschillend beleid voeren.

Dit vraagt om nationaal beleid, uiteraard met het besef dat een en ander zich afspeelt binnen kaders die internationaal en binnen Europa moeten worden afgesproken. Hier ligt een regietaak voor de Rijksoverheid.

Het politieke niveau

Een kerntaak van de nationale overheid is het borgen van de nationale veiligheid. Maar de overheid heeft ook een taak als hoeder van de publieke kennisinfrastructuur. Dit vraagt om het in evenwicht brengen van nationale veiligheidsbelangen en academische belangen. Beide zijn belangrijk.

Het is aan de nationale overheid om de kaders vast te stellen waarbinnen kennisinstellingen beleid dienen te formuleren ten aanzien van de zes genoemde aspecten. Om die kaders te bepalen, is het zaak om diverse schijnbaar tegengestelde belangen in te schatten en tegen elkaar af te wegen. Dat is ingewikkeld. Aan de ene kant van de balans staan de nationale veiligheidsbelangen. Deze kunnen gediend zijn bij terughoudendheid ten aanzien van het participeren in ‘gevoelig’ onderzoek en samenwerking met internationale partners. Die lijn komt soms naar voren in de berichtgeving: civiele kennisinstellingen houden zich verre van militair onderzoek. In sommige gevallen kan het bijdragen aan dit gevoelige onderzoek of het samenwerken met buitenlandse partners echter wel waardevol zijn, bijvoorbeeld omdat dit juist bijdraagt aan nationale veiligheid of de verbetering van internationale verhoudingen. Aan de andere kant van de balans staan tal van andere belangen, zoals vrije wetenschap, economische ontwikkeling en concurrentiekracht, de internationale positie, excellente wetenschap en het aantrekken van kenniswerkers, de aanpak van maatschappelijke uitdagingen of het bijdragen aan *global public goods*.

Het tegen elkaar afwegen van schijnbaar tegengestelde belangen is een ingewikkelde taak. Dit zagen we eerder al bij de steeds nauwere samenwerking tussen universiteiten en bedrijven (Tjong Tjin Tai et al., 2018). Hiervoor is een integraal kader nodig dat de verschillende partijen helpt om weloverwogen te beslissen over welke samenwerkingen wel of niet wenselijk zijn, en welke voorwaarden daarbij passen. Concreet zouden door de politiek vastgestelde kaders een antwoord moeten geven op vragen als: is het verantwoord om samen te werken met een bedrijf als Huawei?[11] Op welke manier moeten studenten en medewerkers uit landen als China en Iran gescreend worden? Aan welke cybersecuritystandaarden moet worden voldaan bij de uitrol van een 5G-netwerk, de ontwikkeling van zelfrijdende auto’s en het gebruik van drones?

---

11 Het feit dat in het VK Oxford University de beslissing heeft genomen om fondsen van dit bedrijf te weren, zonder dat de nationale overheid daarover een standpunt heeft ingenomen, is opmerkelijk.

Uiteraard speelt hier de internationale dimensie een belangrijke rol, aangezien veel van deze kaders internationaal en binnen Europa moeten worden afgesproken. Denk aan de Europese onderzoeksfondsen voor defensie en veiligheid of Europese regelgeving op gebied van cybersecuritystandaarden. Ook internationaal kan Nederland zich hardmaken voor een maatschappelijk verantwoorde kennisontwikkeling voor defensie en veiligheid, bijvoorbeeld door te pleiten voor internationale afspraken die helpen om een potentiële digitale wapenwedloop te monitoren, te reguleren en te de-escaleren.[12]

Het niveau van de kennisinstellingen
Ook kennisinstellingen staan voor de opgave om belangen tegen elkaar af te wegen bij het bepalen van hun beleid op de zes aspecten. Enerzijds zijn ze de vaandeldragers van de vrije wetenschap. Vaak staan ze in een traditie van principiële normen als ‘niet schaden’ en ‘werken in het algemeen belang’. Anderzijds zijn ze, als onderdeel van de Nederlandse maatschappij, ook mede verantwoordelijk voor welzijn en veiligheid van deze samenleving.

Binnen de kaders die nationaal worden vastgesteld is het aan de kennisinstellingen om handen en voeten te geven aan beleid op de zes zojuist besproken aspecten die raken aan defensie en veiligheid. Daarbij kan het gaan om de ontwikkeling en implementatie van regels en procedures, de vaststelling van professionele gedragscodes en de instelling van organen die zich bezighouden met veiligheidsaspecten. Dit kan leiden tot een combinatie van harde en zachte waarborgen, van toetsings- en toestemmingsprocedures voor potentieel gevoelig onderzoek tot het faciliteren van escalatiepaden voor situaties waarin een onderzoeker reden tot zorg voelt.

Het niveau van de individuele onderzoeker
Gezien de veranderende veiligheidssituatie rijst de vraag hoe naïef je als onderzoeker nog mag zijn. Wetenschappers dragen verantwoordelijkheid voor een zorgvuldige omgang met kwesties waar een veiligheidsrisico aan kleeft. Van individuele onderzoekers mag daarom alertheid worden verwacht: een tijdig aankaarten van zaken met een potentieel veiligheidsrisico, of het nou gaat om de inhoud van het onderzoek, of om communicatie, samenwerking, financiering of andere aspecten. Ook is het van belang dat onderzoekers hun kennis en zorgen inbrengen in het publieke debat.

Deze verantwoordelijkheid is te omvangrijk om alleen op de schouders van de individuele onderzoeker te laten rusten. Onze bevindingen laten zien dat kennisontwikkeling voor defensie en veiligheid zich kenmerkt door een complexe

12 Zie Rathenau Instituut (2019), ‘Cyberspace zonder conflict’.

mix van belangen en waarden. Van individuele onderzoekers kan daarom niet worden verwacht dat zij zelfstanding tot weloverwogen beslissingen komen. Bovendien biedt het geen oplossing voor gevallen waarbij de onderzoeker zelf slechte intenties heeft. Het maken van de juiste afwegingen mag dus niet volledig op het bord van de individuele onderzoeker liggen.

5.3 Benodigde vervolgstappen

De politiek en kennisinstellingen kunnen op verschillende thema's beleid formuleren – we presenteerden er zes. De uitwerking en implementatie van dit beleid vragen om inspanningen van de overheid, de instellingen en de individuele wetenschappers. Hoe dit onder de huidige omstandigheden vorm moet krijgen, is een ingewikkeld vraagstuk.

Met betrekking tot de *inhoud van het onderzoek* zelf – de eerste van de zes beleidsthema's – was de praktische gang van zaken vroeger tamelijk simpel. Er werd minder civiel onderzoek verricht dat perspectief bood op militaire toepassingen, en het onderzoek dat in die categorie viel, was redelijk eenvoudig te identificeren. Het ging veelal om biologisch, chemisch, radioactief en nucleair (BCRN) onderzoek op hogere TRLs (technology readiness levels). Voor dat onderzoek bestaan regels die voorschrijven hoe om te gaan met onderzoek of ontwikkelwerk dat zich kenmerkt door dual-use. Deze regels bepalen dat er verscherpte procedures gevolgd moeten worden indien speur- en ontwikkelwerk naast een civiele, mogelijke ook een militaire toepassing opleveren – en dan specifiek een toepassing waarmee schade kan worden toegebracht. Is dat het geval, dan gelden er beperkingen ten aanzien van hoe informatie en kennis gedeeld mogen worden, met wie mag worden samengewerkt en wat er aan resultaten wel of niet de grens over mag. Wanneer onderzoek en ontwikkelwerk tot een product leiden, is er een exportvergunning vereist. Deze arrangementen zijn ook vandaag de dag nog relevant, zoals we in hoofdstuk 2 lieten zien aan de hand van de besproken discussie rondom het volgelgriepvirus van Fouchier en de kennisembargo's ten opzichte van Noord-Korea. Maar dergelijke arrangementen zijn niet ontworpen met het oog op de digitale samenleving. Onze analyse toont aan dat de toepassing van deze regels rond dual-use niet toereikend zijn in de huidige context.

Een van de reden hiervoor is dat veel meer onderzoek dual-use *is* dan vroeger. In de eerste plaats omdat er - naast BCRN - meer typen onderzoek zijn die potentieel militaire toepassingen hebben. Dit geldt met name op het gebied van informatica, kunstmatige intelligentie en robotica. In de tweede plaats zijn kennistoepassingen op lagere TRLs tegenwoordig vaker van mogelijk militaire betekenis.

In een wereld waarin we geen duidelijk onderscheid kunnen maken tussen militaire en civiele kennisontwikkeling, biedt de binaire karakterisering van wel of geen dual-use te weinig houvast om te kunnen omgaan met civiel onderzoek dat militaire betekenis heeft. Bovendien zijn er naast kwesties rondom de inhoud van het onderzoek nog vijf andere, die niet allemaal worden geadresseerd door regels rond dual-use. Het is dus noodzakelijk dat er andere of aanvullende regels komen.

Voor ons ligt dus de uitdaging om procedures te ontwikkelen die helpen om verantwoord te kunnen omgaan met activiteiten met een mogelijk militaire betekenis. Dit zou bijvoorbeeld kunnen betekenen dat defensie- en veiligheidsaspecten een standaard onderdeel worden van de besluitvorming en monitoring rond onderzoeksprocessen – van beoordeling van een voorstel tot evaluatie van proces en resultaat. Hoe een en ander vorm te geven, is nog in ontwikkeling. Bij te ontwikkelen procedures gaat het wellicht niet zozeer om de afweging iets wel of niet te doen (bijvoorbeeld het uitvoeren van een bepaald onderzoek, het aanstellen van een bepaalde medewerker, het aangaan van een samenwerking, het accepteren van financiering uit een bepaalde bron), als wel om het zoeken naar de voorwaarden waaronder iets gedaan kan worden. Niet ja of nee, maar ‘ja, mits…’, of ‘nee, tenzij….’. Ook het institutionaliseren van waarborgen is belangrijk. Het kan bijvoorbeeld relevant zijn om beperkingen op te leggen, vooraf een screening uit te voeren of toezicht te houden tijdens het proces. Soms zal het gaan om het aanmoedigen of ontmoedigen van bepaalde praktijken. Andere situaties vragen om het stellen van context-specifieke voorwaarden.

De procedures die in de loop van de tijd zijn ontwikkeld rondom ethische vraagstukken kunnen dienen als bron van inspiratie voor de omgang met aspecten van defensie en veiligheid. Denk aan ethische gedragscodes, ethische commissies en ethische toetsingsprocedures. Analoog zouden gedragscodes, commissies en toetsingsprocedures voor veiligheid in het leven geroepen kunnen worden. Onderzoekers zouden er terechtkunnen voor advies, en zouden in sommige gevallen verplicht toestemming moeten vragen om bepaald onderzoek te mogen uitvoeren. Het is voor civiele kennisinstellingen mogelijk ook interessant om te kijken hoe publieke kennisorganisaties zoals TNO, MARIN en NLR de omgang met dilemma’s rond veiligheid hebben geïnstitutionaliseerd. Zij combineren van oudsher militaire en civiele kennisontwikkeling binnen één instituut. Ook in Duitsland is inspiratie te vinden; hier hebben veel universiteiten commissies voor *ethical conduct of security-relevant research* ingesteld. Deze commissies implementeren regels en adviseren onderzoekers. Ook hebben ze een rol in het creëren van bewustzijn, ondersteunen ze trainingsmogelijkheden voor onderzoekers en brengen ze kennis over juridische aspecten van onderzoek in. De Duitse tegenhangers van de KNAW en de VSNU ondersteunen deze commissies door het coördineren, signaleren, leren, aggregeren en agenderen van relevante kennis.

Bij het afwegen van nationale veiligheidsbelangen en academische idealen van wetenschappelijke integriteit en open data tegenover internationale samenwerking kunnen bestaande codes, zoals de Nederlandse, Europese of UNESCO-gedragscodes voor wetenschappelijke integriteit, als uitgangspunt dienen. Op basis van deze codes kunnen de condities waaronder internationale partners werken, en de in Nederland geaccepteerde praktijken worden vergeleken. Substantiële onduidelijkheden of afwijkingen hiertussen kunnen aanleiding vormen voor extra maatregelen of een besluit om niet samen te werken. Ook de Algemene Verordening Begevingsbescherming (AVG) kan houvast bieden in het concreet maken van specifieke voorwaarden en procedures. Zo stelt de AVG strenge eisen aan het anonimiseren van persoonsgegevens voor onderzoeksdoeleinden. Ook classificeert de AVG genetische gegevens (zoals DNA-materiaal) en biometrische gegevens (zoals gezichtsafbeeldingen of vingerafdrukgegevens) als bijzondere persoonsgegevens, met als gevolg een aantal specifieke extra eisen. Ook internationale partners moeten aan die eisen voldoen.

Inspiratie voor nieuwe afwegingskaders en procedures kan daarnaast worden gehaald uit de gedachtevorming rond het concept *Responsible Research and Innovation* (RRI, maatschappelijk verantwoord onderzoek en innovatie). Onderzoek en innovatie zijn maatschappelijk verantwoord als het proces transparant en interactief is, waarbij verschillende maatschappelijke actoren zich gezamenlijk buigen over de (ethische) aanvaardbaarheid en maatschappelijke wenselijkheid van het onderzoeks- en innovatieproces. RRI stelt geen harde kaders voor onderzoek – het is geen snelle, kant-en-klare oplossing voor verantwoord bestuur. In plaats daarvan institutionaliseert het continue reflectie en dialoog als onderdeel van het onderzoeksproces.

5.4 Tot slot

Recente geopolitieke, economische en maatschappelijke ontwikkelingen hebben belangrijke gevolgen voor kennisontwikkeling en innovatie voor defensie en veiligheid. In dit rapport lieten we zien wat de consequenties daarvan zijn voor civiele kennisinstellingen. We constateren dat er een reeks van opgaven ligt op het gebied van beleidsontwikkeling, verdeling en aanvaarding van verantwoordelijkheden, afweging van belangen en bescherming van gekoesterde waarden, en van institutionalisering van manieren om met de ontwikkelingen om te gaan.

De tijd van onbevangenheid is voorbij. Dit besef lijkt ook in Nederland door te dringen: wetenschap en technologie hebben een belangrijke positie in de

Nederlandse Chinastrategie van mei 2019, en het gesprek tussen de verschillende ministeries en (de belangenvertegenwoordigers van) de kennisinstellingen komt op gang. Zo organiseerde het Ministerie van Buitenlandse Zaken in november 2018 een stakeholderbijeenkomst rond het thema wetenschap en veiligheid, en vinden eerste gesprekken plaats tussen de verschillende relevante ministeries, de universiteitsbesturen, de KNAW en de VSNU. Op deze manier zal stap voor stap gewerkt moeten worden aan duidelijke afwegingskaders en procedures, om maatschappelijk verantwoord vorm te geven aan kennisontwikkeling die raakt aan defensie en veiligheid. Dat vraagt om gezamenlijk beleid van overheid en kennisinstellingen. Dit rapport schetst hiervan de contouren en algemene termen. Nu komt het aan op invulling en uitwerking.

Dat wordt geen eenvoudige taak. De oude scheiding tussen militaire en civiele kennisecosystemen uitte zich niet alleen in fysieke barrières. Ook in het denken ontstond een scheiding tussen de militaire en civiele wereld. Defensie heeft van oudsher een wat gesloten cultuur, die niet zonder meer een warm welkom biedt aan buitenstaanders. In de civiele wereld bestaat een zekere weerstand tegen het verrichten van onderzoek met militaire doelstellingen. Ook vandaag de dag leidt deze civiel-militaire kloof regelmatig tot gebrek aan begrip, of zelfs wederzijds wantrouwen.

Illustratief is de discussie rondom de totstandkoming van het Europese Defensiefonds. Vanuit militaire hoek zijn er vooral zorgen dat academici en bedrijven terughoudendheid tonen, en wordt opgeroepen ‘de nobele taak’ van militaire R&D te omarmen (Zubaşcu, 2019). Bezorgde onderzoekers en vredesactivisten waarschuwen juist dat het Defensiefonds bijdraagt aan het escaleren van een wereldwijde wapenwedloop, dat met name de klassieke defensie-industrie een vinger in de pap heeft en dat ethische en politieke controle onvoldoende zijn geborgd (Kelly, 2019).

De oproep van de militaire wereld is begrijpelijk. Veiligheid is een belangrijke maatschappelijke uitdaging van deze tijd, en onze analyse laat zien dat civiel georiënteerde kennisinstellingen een mogelijke betrokkenheid niet bij voorbaat de rug kunnen toekeren. Ook de zorgen van de onderzoekers zijn gepast. De militaire wereld moet oog hebben voor de risico’s van een militarisering van het wetenschappelijke domein. De tijd dat de militaire wereld zich kon terugtrekken achter de gesloten deuren van de militaire kennisecosystemen is voorbij. In de zoektocht naar nieuwe samenwerkingen over de civiel-militaire grens, moeten zij de zorgen van de van oorsprong civiel georiënteerde spelers serieus nemen en ruimte bieden aan politieke en ethische controle.

We eindigen dit rapport dan ook niet met een oproep voor of tegen het mobiliseren van civiele kennisecosystemen voor militaire doelen, maar met de observatie dat er nu een kans ligt om in Nederland vorm te geven aan een maatschappelijk verantwoorde kennisontwikkeling voor defensie en veiligheid. Er is behoefte aan duidelijkheid over de relatie tussen het ministerie van Defensie en de krijgsmacht enerzijds en de civiele publieke kennisinstellingen anderzijds. De komende jaren moet die relatie vormkrijgen in nieuwe afwegingskaders, heldere procedures en duidelijke afspraken. De militaire en de civiele wereld hebben een gedeelde verantwoordelijkheid om hiertoe te komen. Wederzijds vertrouwen en begrip voor elkaars rol zijn daarvoor noodzakelijk.

Literatuurlijst

Arbatov, A. (2014). Collapse of the world order? The Emergence of a Polycentric World and Its Challenges

Australian Government Department of Defence (2014). New program to strengthen defence research. In: AG-DoD 23 julie 2014. https://www.dst.defence.gov.au/news/2014/07/26/new-program-strengthen-defence-research

Bakker, A., Drent, M., & Landman, L. (2016). The Parliamentary Dimension of Defence Cooperation. Den Haag: Clingendael

Bekkers, F., W. Oosterveld & P. Verhagen. Checklist for Collaboration with Chinese Universities and Other Research Institutions. Den Haag: HCSS.

Bekkers, F. & T. Sweijs (2016). Op, neer, en zijwaarts. De militaire dimensie van crisismanagement. Den Haag: HCSS.

Bitzinger, R. & N. Popescu (2017). Defence industries in Russia and China: players and strategies. Paris: Institute for Security Studies.

Bos, H., M. van Eeten & B. Jacobs (2017). Behoud en Versterking Nederlandse Cybersecurity Capaciteit. In: dcypher.nl, 23 november 2017.

Brouwer, E. (2015). Innovatie en het nieuwe denken bij DMO. In: Materieelgezien, 5 juli 2015. https://magazines.defensie.nl/materieelgezien/2015/04/04innovatie

Bureau of Industry and Security (2016). Deemed Exports. Washington D.C.: U.S. Department of Commerce. https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports

Charlet, K (2018). The New Killer Pathogens, Countering the Coming Bioweapons Threat. In: Foreign Affairs Mei/Juni 2018. https://www.foreignaffairs.com/articles/2018-04-16/new-killer-pathogens?cid=nlc-fa_fatoday-20180501

Chivvis, C. (2017). understanding Russian ‘Hybrid Warfare’ and what can be done about it. Washington D.C.: RAND Corporation.

Cops, D (2018). Overheidssteun voor dual-use en militair onderzoek en ontwikkeling – uitdagingen en implicaties voor het Vlaams beleid. Brussel: Vlaams Vredesinstituut.

Davies, B. (2019). Oxford places ban on donations and research grants from Huawei. In: The Guardian, 17 januari 2019. https://www.theguardian.com/technology/2019/jan/17/oxford-places-ban-on-donations-and-research-grants-from-huawei-chinese-national-security

De Boer, J. (2011). Een kleine en kwetsbare instelling: een geschiedenis van de Universiteit Twente, 1961-2011. Enschede: Universiteit Twente.

De Boer, M. (2019). Krijgt Franse onderzeebootbouwer een miljardenorder uit Nederland? In: Trouw, 7 februari 2019. https://www.trouw.nl/home/krijgt-franse-onderzeebootbouwer-een-miljardenorder-uit-nederland-~ab2e9df0/

Deuten, J. (2014). R&D goes global: Policy implications for the Netherlands as a knowledge region in a global perspective. Den Haag: Rathenau Instituut.

DeFrance, O., L. Mampaey. & D. Zandee (2016). Defence Industrial Policy in Belgium and The Netherlands. Parijs: ARES.

De Gruyter, C. (2018). China krijgt meer grip op Europa. In: NRC Handelsblad, 5 juli 2018. https://www.nrc.nl/nieuws/2018/07/05/china-krijgt-meer-grip-op-europa-a1609076

De Spiegeleire, S., T. Sweijs (2017). Artifical Intelligence and the future of defense. Den Haag: HCSS.

Department of Transport (2018). New cyber security standard for self-driving vehicles. In: GOV.UK 19 decmber 2018. https://www.gov.uk/government/news/new-cyber-security-standard-for-self-driving-vehicles

Downs, D. & J. Sharpless (2015). Don't Cut Research Ties With the Military. In: The Chronicle of Higher Education, 17 juli 2015. https://www.chronicle.com/article/Don-t-Cut-Research-Ties-With/231699

Drent, M., Dinnissen, R., Van Ginkel, B., Hogeboom, H., Homan, K., Zandee, D. Meijnders, M. (2014). The relationship between external and internal security: Clingendael Strategic Monitor Project. Den Haag: Clingendael.

Edney-Browne, A. & T. Ruff (2018). Partnerships between universities and arms manufacturers raise thorny ethical questions. In: The Conversation, 15 maart 2018. https://theconversation.com/partnerships-between-universities-and-arms-manufacturers-raise-thorny-ethical-questions-93005

Europese Commissie (2017). Reflection Paper on the Future of European Defence. Brussel: Europese Commissie.

Europese Commissie (2019). European Defence Fund – Factsheet. Brussel: Europese Commissie.

Eaglan, M. (2016). What is the Third Offset Strategy? In: RealClear Defense 15 februari 2016. https://www.realcleardefense.com/articles/2016/02/16/what_is_the_third_offset_strategy_109034.html

Feng, E. & C. Clover. Drone swarms vs conventional arms: China's military debate. In: Financial Times 24 augustus 2017.

Freedberg, S. (2014). Star Wars At Sea: Navy's Laser Gets Real. In: Breaking Defense, 10 december 2014. https://breakingdefense.com/2014/12/star-wars-at-sea-navys-laser-gets-real/

Geveke, H. (2016). Technologische revoluties en Defensie - De gevolgen van nieuwe technologische ontwikkelingen voor de krijgsmacht. Militaire Spektator, 185(7), 288-300.

Gummett, P. & J. Stein (1997). European Defence Tecnology in Transition. Londen: Routledge.

Hamer, J., R. van Est, L. Royakkers, met medewerking van N. Alberts (2019). Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict. Den Haag: Rathenau Instituut

Hasu, M., Leitner, K., Solitander, N., & Varblane, U. (2012). Accelerating the Innovation Race: Do We Need Reflexive Brakes? In M. Hasu, K. Leitner, N. Solitander, U. Varblane, K.-E. Sveiby, P. Gripenberg, & B. Segercrantz (Eds.), Challenging the Innovation Paradigm (pp. 60-88). London: Routledge.

Heirbaut, J (2018). Hypersone raket is te snel voor de verdediging. In: NRC 2 november 2018. https://www.nrc.nl/nieuws/2018/11/02/hypersone-raket-is-te-snel-voor-de-verdediging-a2753744

Hoeneveld, F., 2018 Een vinger in de Amerikaanse pap: Fundamenteel fysisch en defensieonderzoek in Nederland tijdens de vroege Koude Oorlog. Utrecht: Universiteit Utrecht.

Hosselet, L. & N. Schuyffel (2014). Urenco moest zich schamen. In: Volkskrant 25 maart 2014. https://www.volkskrant.nl/nieuws-achtergrond/urenco-moest-zich-schamen~be3efe8a/

Hudson, R. (2018). As 'threat vectors' multiply, US Navy expands its global tech-scouting. In: ScienceBusiness, 19 april 2018. https://sciencebusiness.net/news/threat-vectors-multiply-us-navy-expands-its-global-tech-scouting

Inkster, N. (2017). China's strategy to become the world's strongest cyber power. In: NewStatesman 23 februari 2017. https://www.newstatesman.com/microsites/cyber/2017/02/china-s-strategy-become-world-s-strongest-cyber-power

James, A. (2009). Reevaluating the role of military research in innovation systems: introduction to the symposium. Journal for Technology Transfer, 34, 449-454.

Johnson, K. & E. Groll (2019). The Improbable Rise of Huawei - How did a private Chinese firm come to dominate the world's most important emerging technology? In: Foreign Affairs, 3 April 2019. https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/

Johnston, E. (2018). Kyoto University says no to military-related research despite spike in Defense Ministry funding. In: The Japanese Times, 29 maart 2018. https://www.japantimes.co.jp/news/2018/03/29/national/kyoto-university-says-no-military-related-research-despite-spike-defense-ministry-funding/#.XFGvFrx7mUk

Joske, A. (2018). Picking flowers, making honey – The Chinese military's collaboration with foreign universities. Policy Brief nr.10. Sidney: Australian Strategic Policy Institute.

Karampekios, N., Oikonomou, I. & E. Carayannis (2018). The Emergence of EU Defense Research Policy – From Innovation to Militarisation. Washington D.C.: Springer Publishing.

Kennedy, S (2015). What is Made in China – cirtical questions. Washington D.C.: Center for Strategic and International Studies.

Kharpal, A. (2018). China is building a giant $2.1 billion research park dedicated to developing A.I. In: CNBC 3 januari 2018. https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html

Kik, L. (2018). Marine kijkt reikhalzend uit naar nieuwe orders. In: Maritiem Nederland, 29 oktober 2018. http://www.maritiemnederland.com/achtergrond/marinebouwsector-kijkt-reikhalzend-uit-naar-nieuwe-orders/item3038

KNAW (2008). A Code of Conduct for Biosecurity - Report by the Biosecurity Working Group. Amsterdam: KNAW.

KNAW (2014). International scientific cooperation challenges and predicaments: Options for risk assessment. Amsterdam: KNAW.

Koens, L., Meza, C.C., Faasse, P., & De Jonge, J. (2016). *Feiten & Cijfers - De publieke kennisorganisaties.* Den Haag: Rathenau Instituut.

Krijnsen, M. (2014). Aanjager – Universiteitsfonds Twente motor van de ondernemende universiteit. Enschede: Universiteit Twente.

Laterza, V. (2018). Cambridge Analytica, independent research and the national interest. Anthropology Today 34(10). blz. 1-2.

Lintsen, H. (2012). Tachtig Jaar TNO. Delft: TNO.

Louth, J., C. Moelling (2016). The US Third Offset Strategy and the Future of Transatlantic Defense. Parijs: ARES.

Martinage, R. (2014). Toward a new offset strategy – Exploiting U.S. long-term advantages t orestore U.S. global power projection capability. Washington: Centre for Strategic and Budgetary Assessments.

Mazzucato, M. (2013). The Entrepreneurial State. Debunking Public vs. Private Sector Myths. Londen: Anthem Press.

Minaya, E. (2018). Chinese Acquisitions of U.S. Tech Firms Plummeted in 2017. In: The Wallstreet Journal, 5 januari 2018. https://blogs.wsj.com/cfo/2018/01/05/chinese-acquisitions-of-u-s-tech-firms-plummeted-in-2017/"

Ministerie van Buitenlandse Zaken (2019). Kamerbrief inzake verscherpen toezicht op studenten en onderzoekers uit risicolanden.

Ministerie van Defensie (2016). Strategische Kennis- & Innovatieagenda 2016-2020. Den Haag: Ministerie van Defensie.

Molas-Gallart, J. (2009). Innovation, Defence and Security. In J. Molas-Gallart, The Theory and practice of innovation policy (pp. 249-276).

Morland, H. (2005). Born Secret. Cardozo Law Review, Vol 26, No 4, blz. 1401-8.

Mowery, D. (2012). Defense-related R&D as a model for Grand Challenges technology policies. Research Policy 41(10). blz.1703-1715

Mozur, P. & J. Perlez. China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon. In: New York Times, 22 maart 2017. https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html

Mudde, T. (2018). Waarom onderzoeksgeld aannemen van de tabaksindustrie ongehoord is. In: De Volksrant, 20 januari 2018. https://www.volkskrant.nl/wetenschap/waarom-onderzoeksgeld-aannemen-van-de-tabaksindustrie-ongehoord-is~ba77f0e9/

Munnichs, G., M. Kouw & L. Kool (2017). Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut.

Nature (2018). Editorial: Military work threatens science and security. Nature, Vol 556, No 273.

Noort, van W (2018). Nederland kampt met braindrain in artificiële intelligentie. In: NRC 27 augustus 2018. https://www.nrc.nl/nieuws/2018/08/27/nederland-kampt-met-ai-braindrain-a1614393

Overgoor, R., R. van der Lande, H. de Jong & P. Janssen (2018). Economische Effecten Marinebouwcluster. Den Haag: Triarii.

Paillard, C-A., N. Butler (2016). Today's technological innovation for tomorrow's defence. Parijs: ARES.

Pelgrim, C. (2019). KPN kiest omstreden Huawei voor antennes van 5G-netwerk. In: NRC Handelsblad, 26 april 2019. https://www.nrc.nl/nieuws/2019/04/26/kpn-kiest-omstreden-huawei-voor-g5-netwerk-a3958252

Pieke, F., I. d' Hooghe, A. Montulet & M. Wolff (2018). China's rol in internationale onderzoeks- en onderwijssamenwerking. Leiden: LeidenAsiaCentre.

Polyakova, A. (2018). Military-industrial complexities, university research and neoliberal economy. Weapons of the weak: Russia and AI-driven asymmetric warfare. Washington D.C.: Brookings Institute.

Rappert, B., & Balmer, B. (2008). Science, Technology and the Military: Priorities, Preoccupations and Possibilities.

Researchers for Peace (2017). Online pledge to call on the European Union to stop funding military research programmes. https://www.researchersforpeace.eu/researchers-peace

Reich, E. (2011). Science after 9/11: How Research Was Changed by the September 11 Terrorist Attacks. In: Scientific American 1 september 2011.

Sample, I. (2017). Ban on killer robots urgently needed, say scientists. In: The Guardian, 13 November 2017. https://www.theguardian.com/science/2017/nov/13/ban-on-killer-robots-urgently-needed-say-scientists

Schulze, D. (2014). The Civil Clause – A specter is haunting Germany. http://encuentro5.org/home/civilclause

Seligman, L. (2018). The U.S. Defense Department and big tech need each other—but getting along won't be easy. In: Foreign Policy 12 september 2018. https://foreignpolicy.com/2018/09/12/why-the-military-must-learn-to-love-silicon-valley-pentagon-google-amazon/

Shalal, A. (2018). Researchers to boycott South Korean university over AI weapons work. In: Reuters, 4 April 2018. https://www.reuters.com/article/tech-korea-boycott/researchers-to-boycott-south-korean-university-over-ai-weapons-work-idUSL2N1RH0KM

Simonite, T. (2017). Defense Secretary James Mattis Envies Silicon Valley's AI Ascent. In: Wired, 8 november 2017. https://www.wired.com/story/james-mattis-artificial-intelligence-diux/

Spoelstra, J. (2016). Het schip als één systeem. In: Maritiem Nederland, 8 december 2016. http://www.maritiemnederland.com/techniek-innovatie/het-schip-als-een-systeem/item2102

Smart, B. (2016). Military-industrial complexities, university research and neoliberal economy. Journal of Sociology.

Stam, B. (2017). Onbemande schepen: de beste stuurlui staan aan wal. In: Maritiem Nederland, 17 juni 201. http://www.maritiemnederland.com/techniek-innovatie/onbemande-schepen-de-beste-stuurlui-staan-aan-wal/item2299

Temperton, J. (2017). 'Now I am become Death, destroyer of worlds'. The story of Oppenheimer's infamous quote. In: Wirded, 9 augustus 2017. https://www.wired.co.uk/article/manhattan-project-robert-oppenheimer

The Economist (2018). Editorial: How does Chinese tech stack up against American tech? In: The economist, 18 februari 2018. https://www.economist.com/news/business/21737075-silicon-valley-may-not-hold-its-global-superiority-much-longer-how-does-chinese-tech

The Economist (2014). Editiorial: Russia's military modernisation: Putin's new model army. In: the economist, 24 mei 2014. https://www.economist.com/europe/2014/05/24/putins-new-model-army

Tokmetzis, D. & M. Goslinga (2017). How billions vanish into the black hole that is the security industry. In: De Correspondent, 22 february 2017. https://thecorrespondent.com/6229/how-billions-vanish-into-the-black-hole-that-is-the-security-industry/303333613-52f43e22

Vervaeke, L. (2019). De technologische Koude Oorlog. In: De Groene Amsterdammer, 23 januari 2019. https://www.groene.nl/artikel/de-technologische-koude-oorlog

Van Huizen (2017). Onbemand mijnen jagen. In: Maritiem Nederland, 1 november 2017. http://www.maritiemnederland.com/techniek-innovatie/onbemand-mijnen-jagen/item2469

Van Baal, M. (2014). We delen de technische risico's met de markt. In: Maritiem Nederland, 20 november 2014. http://www.maritiemnederland.com/achtergrond/we-delen-de-technische-risico-s-met-de-markt/item1511

Volkskrant (2019), Huawei mogelijk betrokken bij Chinese spionage in Nederland. In: De Volkskrant, 16 mei 2019. https://www.volkskrant.nl/nieuws-achtergrond/huawei-mogelijk-betrokken-bij-chinese-spionage-in-nederland~b4fadc1c/

Wallace, N. (2019). Commission kicks off €500M defence industry programme and publishes €25M defence research calls. In: ScienceBusiness 19 maart 2019.

WRR (2017). Veiligheid in een wereld van verbindingen - een strategische visie op het defensiebeleid. Den Haag: Wetenschappelijke Raad voor Regeringsbeleid.

Bijlage 1

Oriënterende gesprekken

Auke Venema & J.C. Dicke	Ministerie van Defensie
Frank Bekkers	HCSS
Margriet Drent & Dick Zandee	Clingendael

Interviews casestudy

Marnix Krikke	Netherlands Maritime Technology
Chris van den Berg	Ministerie van Defensie
Bas Buchner	MARIN
Peter van Terwisga & Willem Laros	Damen Shipyards
Hans Hopman	TU Delft
Hendrik-Jan van Veen	TNO
Wik Jongsma	Thales

Open Access
Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

Contactgegevens
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut