Innovatie in de schaduw: de strijd van geheime diensten

Rietjens, S.J.H.

Prof.dr.ir. Sebastiaan J.H. Rietjens

Innovatie in de schaduw: de strijd van geheime diensten

Universiteit Leiden

Bij ons leer je de wereld kennen

Innovatie in de schaduw: de strijd van geheime diensten

Oratie uitgesproken door

Prof.dr.ir. Sebastiaan J.H. Rietjens

bij de aanvaarding van het ambt van bijzonder hoogleraar
Intelligence in War and Conflict
aan de Universiteit Leiden
op vrijdag 5 juli 2024.

Universiteit
Leiden

Geachte Rector, beste collega's, familie en vrienden, zeer gewaardeerde toehoorders,

Q-day is de dag waarop quantumcomputers sterk en stabiel genoeg zijn om onze huidige computerbeveiliging te kraken. Dat klinkt best eng, toch? Stel je voor: de Rotterdamse haven die platligt, het energienetwerk dat hapert, of het digitale betalingssysteem dat ineens niet meer werkt. Dat zijn echte doemscenario's.
Onze inlichtingen- en veiligheidsdiensten, ook wel bekend als geheime diensten, zijn druk bezig om zich voor te bereiden op Q-day. Ze willen niet alleen de risico's aanpakken, maar ook de kansen verkennen die een nieuwe technologie zoals *quantum* biedt. Dat betekent dat ze moeten vernieuwen: in hun werkwijze, de technologie die ze gebruiken en het personeel dat ze in dienst hebben. Deze vernieuwingen staan ook wel bekend als innovatie.

Leidinggevenden bij de diensten hameren constant op het belang van innovatie. Jan Swillens, de voormalig directeur van de Nederlandse Militaire Inlichtingen- en Veiligheidsdienst, de MIVD, zei het zo: "Werken in een context van continue verandering is onze *core business*. De ontwikkelingen volgen elkaar in hoog tempo op. Dus continue innoveren en verbeteren is onze realiteit." En zoals een échte militair betaamt, sloot hij af met de wijsheid: "Stilstand is achteruitgang"[1].

Het is daarom best verrassend dat we eigenlijk niet precies weten hoe inlichtingen- en veiligheidsdiensten nu écht innoveren en welke uitdagingen ze tegenkomen. Hun mysterieuze imago kan innovatie flink in de weg zitten, vooral wanneer ze samenwerken met externe partijen.
Als we eens duiken in het wetenschappelijke domein van inlichtingenstudies, dan blijkt dat het thema innovatie zo goed als vergeten is. Steve Coulthart en Abebe Rorissa hebben een berg van meer dan 6000 publicaties doorgespit en wat blijkt? Innovatie komt maar sporadisch aan bod[2]. Binnen de diensten zelf is de kennis over innovatie vaak ook beperkt. Ze focussen vooral op veranderingen in de buitenwereld, zoals de opkomst van desinformatie[3] of de rol van de private sector[4]. Maar wat dat voor henzelf betekent, blijft vaak onderbelicht. En als ze er al over praten, gaat het meestal alleen over technologische innovatie, terwijl andere vormen van innovatie, zoals hoe ze hun zaken intern regelen, over het hoofd worden gezien[5].

In deze oratie ga ik het hebben over hoe inlichtingen- en veiligheidsdiensten innoveren en welke uitdagingen ze daarbij tegenkomen. Ik heb mijn oratie in drie delen opgedeeld. In het eerste deel leg ik uit wat we onder innovatie verstaan, bespreek ik belangrijke innovatiegebieden en introduceer ik het concept 'innovatievermogen' uit de organisatiekunde. In het tweede deel analyseer ik hoe inlichtingen- en veiligheidsdiensten innoveren en welke obstakels ze daarbij ervaren, gezien vanuit het perspectief van innovatievermogen. Hierbij focus ik op zes factoren die in de literatuur worden genoemd en essentieel zijn voor een organisatie om te innoveren. Ik baseer me daarbij op literatuur, beleidsdocumenten, en talloze interviews die ik en mijn studenten hebben afgenomen bij medewerkers van verschillende diensten. In het derde deel presenteer ik de grote lijnen van mijn onderzoeksagenda en sluit ik af.

Innovatie
Innovatie is een complex fenomeen. Hoewel er duizenden publicaties zijn over innovatie in de organisatieliteratuur, bestaat er geen consensus over de precieze definitie ervan. Over het algemeen gaat het bij innovatie om iets nieuws. Dit kan een proces of een product zijn. Daarnaast kan het vernieuwende aspect zowel relatief als absoluut zijn, en kan de innovatie abrupt of juist geleidelijk worden ingevoerd. Voor inlichtingen- en veiligheidsdiensten definieer ik innovatie als elke verandering in hun werkwijze, waarbij zij gebruik maken van nieuwe processen, concepten, en/of resulterend in nieuwe producten of diensten[6].

Binnen het inlichtingen- en veiligheidsdomein vinden er verschillende soorten innovatie plaats. Technologische innovatie

springt het meest in het oog[7]. Denk hierbij aan ontwikkelingen op het gebied van biotechnologie, radartechnologie en kunstmatige intelligentie. Een concreet voorbeeld van technologische innovatie in het inlichtingenproces is de automatische aansturing van satellieten. Bij het waarschuwen voor een Russische inval in de Oekraïne in 2022 speelden satellietbeelden een cruciale rol. Hoewel het nuttig was om te weten dat Russische tanks en luchtafweersystemen werden ingezet op locaties die voorheen verlaten waren, zorgde de overvloed aan informatie ervoor dat Westerse inlichtingenanalisten werden overspoeld. Machine learningtoepassingen stelden satellieten in staat om automatisch de ontwikkelingen van het Russische leger te monitoren. Zo konden inlichtingendiensten de besluitvormers tijdig informeren over de precieze locatie van Russisch materieel vóór de invasie[8].

Een tweede gebied waar innovatie plaatsvindt, betreft de inlichtingenmethoden. Bij het inwinnen van gegevens wordt steeds meer aandacht besteed aan non-verbale communicatie. Zo kunnen gezichtsuitdrukkingen en lichaamsbewegingen bij ondervragingen waardevolle inzichten opleveren. Daarnaast worden er steeds meer nieuwe analysetechnieken toegepast. Een bekend voorbeeld zijn de zogenaamde *structured analytic techniques*. Denk hierbij aan methoden zoals de *Alternative Futures Analysis*, sociaal netwerkanalyse en de door mijn collega Peter de Werd ontwikkelde methode *Analysis by Contrasting Narratives* (ACN)[9].

Het derde en laatste gebied waarop innovatie plaatsvindt heeft betrekking op de diensten zelf. Hier zien we vernieuwing op het vlak van human resources, IT-infrastructuur, organisatiestructuur, en huisvesting. Zo zet de MIVD momenteel fors in op het verbeteren van de werving van nieuwe medewerkers en investeert zij in strategisch talentmanagement, o.a. door het vrijmaken van personeel voor promotieonderzoek[10].

Hoewel vaak wordt gesuggereerd dat innovatie afhankelijk is van de sector, de industrie of de organisatie, toont de organisatiekundige literatuur aan dat het zogenaamde 'innovatievermogen' van een organisatie bepalend is voor effectieve innovatie. Dit vermogen houdt in dat een organisatie voortdurend kennis en ideeën kan omzetten in nieuwe producten, processen en systemen die ten goede komen aan de organisatie[11]. Hoewel dit concept oorspronkelijk is ontwikkeld voor de private sector, is het ook uitgebreid onderzocht en toegepast in verschillende publieke sectororganisaties zoals ziekenhuizen[12] en lokale overheidsinstanties[13].

Het vaststellen van het innovatievermogen van organisaties is een uitdagende taak. De belangrijkste factoren zijn vaak pas achteraf te identificeren en het gaat om een complex samenspel van verschillende elementen die van geval tot geval kunnen variëren[14]. Ondanks deze uitdagingen komt zowel uit de organisatiekundige literatuur als praktijkervaringen naar voren dat er zes cruciale factoren zijn voor het innovatievermogen van een organisatie[15]. In het volgende deel van deze oratie zal ik deze zes factoren verder verkennen in het domein van de inlichtingen- en veiligheidsdiensten.

Factor 1: een heldere visie en strategie

Een gezamenlijke visie en strategische aansturing zijn essentieel voor innovatie. Ze bepalen namelijk hoe organisaties hun middelen, producten, processen en systemen inzetten om met hun omgeving om te gaan[16].

Het analyseren van de innovatiestrategie en -visie van de diensten is geen eenvoudige opdracht. De meeste strategiedocumenten zijn gerubriceerd en alleen intern beschikbaar. Soms onthullen organisaties delen van hun visie of strategie tijdens toespraken of in jaarverslagen. In een recente *keynote speech* benadrukte Jennifer Ewbank, plaatsvervangend directeur van de CIA, dat "innovatie, risico nemen, experimenteren en slim falen niet alleen de beste weg vooruit is, maar voor degenen die verantwoordelijk zijn voor de nationale veiligheid in Amerika, zelfs de enige weg vooruit"[17]. Ook de eerdergenoemde uitspraak van Jan Swillens, "stilstand is achteruitgang", sluit hier goed bij aan.

Helaas blijven deze uitspraken vrij abstract en gaan ze niet veel verder dan het belang van innovatie te benadrukken. Steve Blank[18] is hier kritisch over en stelt dat "ondanks dat alle inlichtingenorganisaties je willen doen geloven dat innovatie een van hun pijlers is, blijkt innovatie in de praktijk vaak vaag en slecht gedefinieerd te zijn terwijl er veel middelen aan worden besteed".

Om deze kritiek te ondervangen, heeft de MIVD in 2022 een innovatiestrategie opgesteld. Deze 'Innovatie Agenda' definieert de innovatiedoelen van de dienst en identificeert verschillende maatregelen om het innovatievermogen te vergroten. Denk hierbij aan gerichte sturing van innovatie-activiteiten, toewijzing van financiële middelen om innovatie te stimuleren, en het versterken van samenwerking met andere onderdelen van het Ministerie van Defensie, kennispartners en de private sector.[19] Daarnaast geeft de Innovatie Agenda prioriteit aan bepaalde technologieën waarop de MIVD verder wil innoveren, zoals kunstmatige intelligentie, biometrie en het eerdergenoemde *quantum computing*.

Factor 2: competentiebasis

Het goed benutten van de aanwezige competenties is essentieel voor innovatie in een organisatie. Ik zal me richten op vier belangrijke aspecten: samenwerkingsverbanden, diversiteit, expertise en leiderschap.

Samenwerking leidt vaak tot nieuwe ideeën en impulsen. Voor inlichtingen- en veiligheidsdiensten zijn de belangrijkste partners van oudsher andere diensten[20], maar tegenwoordig in toenemende mate ook academische instellingen[21], en de private sector[22]. De directeur van de Britse Secret Intelligence Service benadrukte het belang van samenwerking met de tech-industrie: "We kunnen de mondiale tech-industrie niet meer kopiëren; laten we er dus zo goed mogelijk gebruik van maken"[23]. Het onderhouden van samenwerkingsverbanden blijkt een grote uitdaging voor diensten, vooral omdat ze van nature afgeschermd zijn. Vaak wordt er aandacht besteed aan de formele samenwerkingsstructuren en gaat samenwerking uit van wederkerigheid. Het bekende principe van *Quid pro Quo*. Maar uitgebreid onderzoek door Pepijn Tuinier[24] laat zien dat wederzijds vertrouwen en sociale relaties minstens zo belangrijk zijn. Banden tussen inlichtingenprofessionals zijn gebaseerd op reputatie, professioneel respect en gedeelde normen en waarden. Deze banden zorgen ervoor dat de brug kan worden geslagen tussen medewerkers uit verschillende landen, organisaties of zelfs tussen mensen met tegenstrijdige belangen. Op de conferentie van de Nederlandse Inlichtingen Studies Associatie (NISA) afgelopen oktober stelde de directeur van de MIVD: "inlichtingen en veiligheidsorganisaties moeten op een slimme manier samenwerken om hun concepten, werkwijzen en technologie op peil te houden"[25]. Hoewel dit veelbelovend klinkt en het personeel aanmoedigt om naar buiten te treden, blijft het onduidelijk wat die slimme manier precies inhoudt en hoe samenwerking daadwerkelijk kan worden gestimuleerd.

Diversiteit is een tweede belangrijk aspect voor een sterke competentiebasis. Culturele diversiteit wordt vaak gezien als de voornaamste uiting van diversiteit en is gebaseerd op religie, etniciteit, gender, leeftijd of sociaal-economische achtergrond. Maar daarnaast is ook cognitieve diversiteit van groot belang[26]. Matthew Syed stelt in zijn boek '*Rebel Ideas*' dat complexe inlichtingenproblemen vanuit verschillende perspectieven moeten worden bekeken om vooroordelen en traditionele denkpatronen te vermijden[27]. Het falen van de Amerikaanse CIA bij het herkennen van signalen voorafgaand aan de aanslagen van 9/11 wordt mede toegeschreven aan de homogeniteit van het personeelsbestand dat overwegend bestond uit blanke mannen met een diploma van een Ivy League universiteit.

Een sterke competentiebasis vereist expertise op de gebieden waarop wordt geïnnoveerd. Dit hangt nauw samen met cognitieve diversiteit. In de meeste inlichtingen- en veiligheidsdiensten is bèta-geschoold personeel schaars, terwijl technologische innovaties juist essentieel zijn. Diensten moeten daarom initiatieven nemen om technisch personeel aan te nemen en te

behouden. Een mooi voorbeeld hiervan is de jaarlijkse *summer school* van de Joint Sigint Cyber Unit[28].

Tot slot is leiderschap een cruciaal aspect van de competentiebasis van een dienst. Leiderschap speelt een belangrijke rol bij het vergroten van de creativiteit van een organisatie, en het overwinnen van weerstand binnen en buiten een organisatie[29]. Arthur Docters van Leeuwen is hierbij een goed voorbeeld. Hij was van 1989 tot 1995 het diensthoofd van de Binnenlandse Veiligheidsdienst (BVD), de voorloper van de AIVD. Dit was de tijd waarin de Sovjet-Unie uiteenviel en het terrorisme opkwam. Deze veranderingen vroegen om een nieuwe manier van werken. Onder leiding van Docters van Leeuwen moderniseerde de BVD op veel terreinen en bracht de dienst het eerste publieke jaarverslag uit onder het motto: "open waar het kan, gesloten waar het moet"[30].

Factor 3: Organisatie leervermogen

De organisatieliteratuur onderscheidt verschillende soorten leren. Ten eerste kennen we '*single loop learning*', wat verwijst naar het doen van relatief eenvoudige aanpassingen en correcties. Dit wordt ook vaak gezien als kort-cyclisch innoveren. '*Double loop learning*' betekent dat we onderwerpen op een nieuwe manier gaan zien. Tot slot, bestaat er '*triple loop learning*', waarbij actoren nieuwe processen of methoden ontwikkelen om tot deze nieuwe zienswijzen te komen[31]. De laatste twee vormen van leren vallen onder lang-cyclisch innoveren. Op het niveau van *single loop learning* zien we duidelijke voorbeelden binnen inlichtingen- en veiligheidsdiensten. Op individueel en teamniveau vindt het leren doorlopend plaats. Medewerkers maken steeds vaker gebruik van openbare bronnen en data-analisten experimenteren met beschikbare software en modellen. Op organisatieniveau zijn er echter vaak weinig formele procedures om ervaringen en geleerde lessen vast te leggen. Sommige medewerkers documenteren hun ervaringen en lessen wel (vaak in zelfontwikkelde formats), terwijl anderen hier minder aandacht aan besteden. Dit leidt tot fragmentatie en belemmert een structurele vergelijking en analyse van geleerde lessen.

Daarnaast geven leidinggevenden vaak de voorkeur aan operationeel inzetbaar personeel boven personeel dat verantwoordelijk is voor het vastleggen en documenteren van opgedane kennis. Hoewel dit begrijpelijk is vanuit een operationeel perspectief, komt het lerend vermogen van een organisatie hierdoor in het gedrang. Tot slot speelt psychologische veiligheid een belangrijke rol bij het lerend vermogen. Dit houdt in dat medewerkers kritisch kunnen zijn naar zichzelf, hun team en de gehele organisatie, in de verwachting dat collega's en leidinggevenden hier constructief op reageren. Pas als dit gebeurt, kan een organisatie daadwerkelijk leren.

Op het niveau van *double loop learning* zien we een langzame verandering in de benadering van inlichtingenvraagstukken. Kortgezegd betekent dit dat inlichtingenvraagstukken niet langer als oplosbare puzzels worden gezien, maar als complexe mysteries[32]. Het zijn ambigue problemen die niet langer volledig te doorgronden zijn. Een goed voorbeeld hiervan is de manier waarop China onze kennisveiligheid en vitale infrastructuur bedreigt. De Chinese inlichtingenstrategie omvat een '*whole of society*'-benadering. Wereldwijd zijn er naar schatting meer dan 150.000 Chinese staatsbedrijven die actief worden aangestuurd door hun inlichtingendiensten[33]. Deze organisaties omvatten luchtvaart- en technologiebedrijven, onderzoeksinstituten en defensie-organisaties. Ook heeft China een uitgebreid programma om wetenschappelijk toptalent dat buiten China werkt, te rekruteren. Dit '*thousands talents plan*' richt zich op tienduizenden wetenschappers, vaak met een Chinese nationaliteit. Via dit programma vloeit veel intellectueel eigendom terug naar China. Hoewel de meeste van deze wetenschappers in de VS werken, is ongeveer 10% in Europa actief is. Nederland stond enkele jaren geleden op de tweede plaats in Europa, met tientallen senior-onderzoekers die aan dit programma waren verbonden[34]. Dit roept vele dilemma's op, zoals bij de toelating van Chinese studenten tot universiteiten of de overname van Nederlandse bedrijven door China. Met andere woorden, er is geen eenduidig beeld.

Nu het besef van deze paradigmaverandering langzaam maar zeker indaalt, wordt het voor inlichtingen- en veiligheidsdiensten steeds belangrijker om nieuwe processen en methoden te ontwikkelen. Dit valt onder het derde niveau van *triple loop learning*. Een van de grote uitdagingen hierbij is het gebruik van open bronnen. Het conflict in de Oekraïne heeft het belang van open bronnen duidelijk aangetoond. Voorbeelden zijn er te over: van Maxar Technologies dat satellietdata verspreidt tot "LiveUAmap" dat bijna live verslag doet van de ontwikkelingen op het slagveld in Oekraïne en deze op een kaart weergeeft[35].
Open bronnen hebben verschillende voordelen. Ze bieden een bredere context voor reeds vergaarde inlichtingen, zijn vaak goedkoper dan andere inlichtingenbronnen en kunnen eenvoudig worden verspreid[36]. De CIA-directeur voor digitale transformatie benadrukte onlangs: "Vandaag de dag zijn open bronnen een van de rijkste beschikbare bronnen en onze eerste keuze in een zeer dynamische en digitale omgeving"[37].
Ondanks het geweldige potentieel van open bronnen en het subsidiariteitsbeginsel dat bepaalt dat inlichtingen- en veiligheidsdiensten het lichtste middel in moeten zetten waarmee een doel bereikt kan worden, lijken open bronnen nog onvoldoende te worden benut. Deels komt dit omdat bijzondere inlichtingenmiddelen vaak hoger in aanzien staan dan open bronnen. Tevens is er de zorg dat intensivering van het gebruik van open bronnen kan leiden tot een afname van het exclusieve karakter van diensten ten opzichte van denktanks, onderzoeksinstituten en organisaties zoals Bellingcat. En, tot slot, aangezien open bronnen niet afgeschermd zijn, is het vaak onduidelijk wat nu precies informatie is en wanneer het om inlichtingen gaat. Hierdoor kan het begrip inlichtingen zijn waarde gaan verliezen of zoals Wilhelm Agrell het 2 decennia geleden al verwoordde: "When everything is intelligence, nothing is intelligence"[38].

Een tweede uitdaging bij de ontwikkeling van nieuwe processen en methoden is de adoptie van het datagedreven werken. Hoewel veel inlichtingenteams voornamelijk traditionele en kwalitatieve analyses gebruiken, worden zij nu geconfronteerd met grote ontwikkelingen in technologie en informatie. Diensten hebben potentieel toegang tot een exponentieel groeiende hoeveelheid data, steeds krachtigere computers en modellen voor data-analyse. Het is essentieel om datagedreven werken te omarmen, maar veel diensten ondervinden hierbij grote uitdagingen. Vaak wordt er direct gewezen naar het kleine aantal medewerkers met een bèta-profiel binnen diensten. Hoewel dit zeker het geval is, zijn er veel andere uitdagingen zoals de beschikbare infrastructuur (o.a. hardware, software en applicaties), data-analfabetisme bij analisten en management, en de integratie van kwalitatieve en kwantitatieve analyses.

Factor 4: Creativiteit en het managen van ideeën.
De vierde factor draait om creativiteit en het managen van ideeën. Creativiteit is essentieel voor organisaties om complexe problemen aan te pakken. Hoewel er enkele studies zijn die het belang van creativiteit voor inlichtingen- en veiligheidsdiensten benadrukken, zijn er maar weinig studies die echt diep ingaan op dit onderwerp. In de praktijk zijn er verschillende manieren waarop diensten creativiteit binnen hun organisaties stimuleren. Zo worden er tal van symposia georganiseerd en hebben sommige diensten specifieke onderscheidingen of competities in het leven geroepen. De Amerikaanse inlichtingengemeenschap kent bijvoorbeeld de *Galileo Awards* om personeel met de meest innovatieve ideeën te belonen[39]. In Nederland organiseert de MIVD een soort '*Dragon's Den*' waar personeel nieuwe ideeën kan pitchen.
Een andere manier om creativiteit te stimuleren is via onderwijs. De laatste decennia zijn er verschillende programma's opgezet voor inlichtingenpersoneel. In de VS kun je bijvoorbeeld studeren aan de *National Intelligence University.* De Nederlandse Defensie Academie heeft mede op verzoek van de MIVD de Master of Military Strategic Studies opgezet, met een sterke inlichtingencomponent.
Een laatste voorbeeld om creativiteit op individueel niveau te ondersteunen is terug te vinden in de *CIA-labs*. Hier kunnen medewerkers patenten aanvragen om hun intellectueel eigendom te beschermen. Dit stelt hen in staat om financieel te profiteren van hun ideeën, in plaats van toe te kijken hoe de private sector daarmee winst maakt[40].

Op organisatieniveau is het opzetten van een Skunkworks-achtig team een goede manier om creativiteit te bevorderen. Deze kleine, losjes gestructureerde groepen richten zich op radicale innovatie. Zij worden zo min mogelijk belemmerd door regelgeving en bureaucratie[41]. De term 'Skunkworks' komt van Lockheed Martin's Skunkwork project uit de Tweede Wereldoorlog, dat heeft geleid tot innovaties zoals de Blackbird, het U2-spionagevliegtuig en het eerste stealth vliegtuig, de F117. De Israelische Shin Bet is hierdoor geïnspireerd en heeft onlangs een *Tech Garage* opgezet, waarbij zij samen met *start-ups* nieuwe technologie en risicovolle initiatieven ontwikkelt en de rigide overheidscultuur probeert te omzeilen[42].
Tot slot realiseren diensten zich steeds meer dat samenwerking met anderen essentieel is om nieuwe ideeën te genereren. Het '*lone genius*'-paradigma, waarbij één genie verantwoordelijk is om een innovatie te realiseren, moet plaatsmaken voor samenwerking. Elon Musk en zijn bedrijf Starlink dat nieuwe communicatiemogelijkheden biedt in de Oekraïne is het bewijs dat individuen nog steeds een impact kunnen hebben, maar complexe innovaties vereisen samenwerking[43].

Alle genoemde initiatieven richten zich vooral op het genereren van nieuwe ideeën. Het vastleggen van die ideeën en het ontwikkelen van oplossingen die daadwerkelijk in diensten kunnen worden toegepast, is echter een ander verhaal. Een positieve uitzondering is het werk van Richards Heuer Jr., die veel inzichten uit de gedragseconomie heeft geïntegreerd in het inlichtingendomein. In zijn bekendste werk, '*The Psychology of Intelligence Analysis*', beschrijft hij het effect van cognitieve vooroordelen zoals groepsdenken of spiegelen. Zijn werk vormde de basis voor de gestructureerde analysetechnieken die we nu kennen in het inlichtingendomein[44].
Over het algemeen blijkt het lastig om de kloof te overbruggen tussen het genereren van ideeën en het daadwerkelijk implementeren van werkende oplossingen. Steve Blank[45] gaat zelfs zo ver om te zeggen: "Accelerators, hubs, cafés, open-sourcing, crowd-sourcing, maker spaces, chief innovation officers, etc. zijn allemaal fantastisch, maar ze creëren een soort innovatietheater. Veel woorden, maar weinig daden. Er worden geweldige demo's gegeven, veel kopjes koffie gedronken en posters gemaakt, maar het eindresultaat valt vaak tegen. De meeste betrokkenen ervaren geen tot weinig verschil door al deze initiatieven."

Een belangrijke onderliggende reden voor het gat tussen creatie en implementatie ligt in de organisatiestructuur van diensten[46]. Dit is de vijfde factor die ik wil bespreken.

Factor 5: Organisatiestructuur
De structuur van een organisatie is cruciaal voor succesvolle innovatie[47]. Innovatieve organisaties vertonen een aantal gemeenschappelijke kenmerken. Zoals ik eerder al besprak, is de relatie met externe partners van groot belang. Creativiteit staat hoog in het vaandel en innovatieve organisaties geven hun personeel de ruimte om te experimenteren en bestaande procedures, normen en prestatiecriteria ter discussie te stellen. De eerdergenoemde Skunkworks-achtige organisaties zijn hiervan een mooi voorbeeld. Dennis Blair, voormalig Amerikaans Director of National Intelligence, beaamt dit en zegt: "Als we onze inlichtingenprofessionals de juiste doelen stellen en alle obstakels uit de weg ruimen, zullen degenen die vertrouwen in hen hebben ook geweldige resultaten terugzien"[48].

Deze kijk lijkt mij te simplistisch voor inlichtingen- en veiligheidsdiensten. Zij zijn van nature bureaucratisch en zowel de politiek als maatschappij verwachten een hoge mate van betrouwbaarheid. Dit soort organisaties hebben daarom veel baat bij stabiliteit. Ze worden gekenmerkt door taakspecialisatie, duidelijke gezagsverhoudingen, een naar binnen gekeerde houding en het formaliseren van processen en voorschriften[49]. Deze kenmerken lijken haaks te staan op de eigenschappen van organisaties die als innovatief worden bestempeld. Het gevolg van deze tegengestelde logica is dat innovatie niet vanzelfsprekend is in de meeste diensten. Het is dus belangrijk om een juiste balans te vinden.

De organisatieliteratuur introduceerde hiervoor het begrip '*ambidexterity*', oftewel het vermogen om twee dingen tegelijkertijd te doen. Vergelijk het met een goede pianospeler die tegelijkertijd met zijn linker- en rechterhand speelt. In de context van innovatie betekent dit dat een organisatie zowel haar reguliere taken moet uitvoeren als nieuwe werkwijzen moet ontwikkelen. Zij moet kunnen concurreren in een stabiele markt waar controle, en kleine verbeteringen belangrijk zijn, maar ook in een opkomende markt waar flexibiliteit, autonomie en experimenten nodig zijn[50].
Empirische studies tonen duidelijk aan dat er organisaties bestaan die deze tweeledige aanpak omarmen en dat dit positieve resultaten oplevert[51]. Er zijn verschillende manieren om *ambidexterity* vorm te geven. Zo heeft structurele *ambidexterity* te maken met de organisatiearchitectuur. De cruciale taak is niet om de organisatie simpelweg op te splitsen in een deel dat zich richt op dagelijkse zaken en een deel dat zich richt op innovatie. Het gaat er juist om deze verschillende onderdelen op een zinvolle wijze te integreren[52].
Cyclische *ambidexterity* betekent dat organisaties een patroon volgen van langdurige stabiliteit en kleine aanpassingen, gevolgd door kortstondige, radicale veranderingen[53]. Deze discussie vindt ook plaats in het inlichtingendomein waar evoluties en revoluties elkaar afwisselen[54].

Een derde benadering is contextuele *ambidexterity*. Hierbij ligt de nadruk op het verschil per context en organisatieniveau. Vooral leidinggevenden moeten in staat zijn om de brug te slaan tussen een innovatieve aanpak en behoudende praktijken[55]. Binnen inlichtingen- en veiligheidsdiensten moeten zij oog hebben voor het runnen van de organisatie en het naleven van wet- en regelgeving, terwijl ze tegelijkertijd innovatie en nieuwe ontwikkelingen moeten stimuleren. Het is verleidelijk om de waan van de dag te laten leiden, want innovatie is vaak inefficiënt en gaat dan ook regelmatig gepaard met slechte ideeën[56]. Een uitgebreide studie naar S&P 500-bedrijven in de VS toont aan dat ongeveer 80% van de onderzochte organisaties onevenredig veel aandacht besteedt aan het draaiende houden van de organisatie ten koste van innovatie[57].

Factor 6: Cultuur
De cultuur van een organisatie speelt een belangrijke rol in het innovatieproces[58], en dat geldt ook voor inlichtingen- en veiligheidsdiensten. Het gezaghebbende CSIS-rapport '*Maintaining the Intelligence Edge*' benadrukt zelfs dat het grootste obstakel voor innovatie niet de technologie zelf is, maar juist de cultuur binnen deze diensten[59]. Laten we eens dieper ingaan op twee culturele kenmerken.

Allereerst weerstand tegen verandering. Dit fenomeen is bekend in de verandermanagementliteratuur, maar krijgt weinig aandacht in de inlichtingenliteratuur. Redenen voor deze weerstand zijn bijvoorbeeld het niet zien van de noodzaak om te veranderen, de kosten die met een verandering gepaard gaan of ervaringen uit het verleden[60].
Net zoals in iedere organisatie, zien we weerstand tegen verandering binnen de inlichtingen- en veiligheidsdiensten op verschillende terreinen terugkomen. De overgang naar een datagedreven organisatie en het intensiever gebruik maken van open bronnen zijn hierbij slechts twee voorbeelden.

Het tweede kenmerk dat opvalt in de cultuur van diensten is risicomijdend gedrag. Hoewel de meeste innovaties veel tijd en inzet vragen, blijven leidinggevenden vaak maar een korte periode in functie. Ze zijn daarom voorzichtig met het toekennen van middelen en tijd aan innovaties, vooral in tijden van bezuinigingen. En op de werkvloer vertrouwen operators en analisten vaak op bewezen technologie en procedures, waardoor nieuwe ideeën en technologie soms moeilijk geaccepteerd worden.

Het is interessant om te zien dat het culturele kenmerk dat inlichtingen- en veiligheidsdiensten onderscheidt van 'doorsnee' organisaties, namelijk geheimhouding, niet uitvoerig is onderzocht[61]. Maar juist dit begrip van geheimhouding heeft grote invloed op het innovatievermogen van diensten. Zoals ik eerder al betoogde, zijn diensten niet langer de dominante partij als het op innoveren aankomt. Ze zijn sterk afhankelijk van externe actoren. Omdat geheimhouding zich per definitie

richt op het afschermen van informatie, kennis en gedrag van anderen, belemmert het de samenwerking.
In sommige gevallen zijn er duidelijke wettelijke richtlijnen over welke informatie wel of niet gedeeld mag worden en met wie. Dit gaat vooral om specifieke doelen, bronnen en methoden. Maar vaak bevinden ze zich in een grijs gebied, waar het niet zo eenvoudig is om de grenzen van een geheim te definiëren. Medewerkers van diensten kiezen dan vaak voor de veilige kant. Eleni Braat[62] verklaart deze praktijk binnen de diensten met het begrip '*goal displacement*'. Dit treedt op wanneer het volgen van de regels een doel op zichzelf wordt[63]. Uiteindelijk vergroot dit de kloof tussen de diensten en de buitenwereld, en vormt zo een drempel voor innovatie.
Paul Oling, die onderzoek doet naar de rol van geheimhouding bij innovatie, tekende in een van zijn interviews met een inlichtingenmedewerker op: "het probleem is dat we zo geheim zijn, waardoor de industrie niet naar ons toekomt met oplossingen. Ze denken dat we bepaalde technologie*ën* al gebruiken. Of ze pushen juist technologie*ën* die we al hebben of die niet aan onze behoeften voldoen". Deze respondent suggereerde dat iemand Tom Clancy maar eens moest vertellen om wat nauwkeuriger te zijn in zijn boeken.

Conclusie
Ik ben nu bij de conclusie aangekomen. Innovatie in het domein van inlichtingen en veiligheid wordt vaak gezien als iets technologisch, disruptiefs en grootschaligs. Maar zoals we hebben gezien, is het eigenlijk veel diverser dan dat. Er vinden momenteel allerlei innovaties plaats die zich richten op de organisatie, de inlichtingenmethoden, en het personeelsbestand. Veel van deze vernieuwingen komen echter traag op gang en zijn relatief beperkt in omvang.

Wat betreft innovatie binnen inlichtingen- en veiligheidsdiensten: daar wordt veel over gesproken, maar diensten voegen vaak maar beperkt de daad bij het woord. Een gebrek aan kennis speelt hierbij een belangrijke rol. Het is vaak onduidelijk welke stappen innovatie precies doorloopt, welke obstakels en dilemma's erbij komen kijken, en hoe diensten hiermee om moeten gaan. Om dit gat in onze kennis te dichten heb ik het begrip 'innovatievermogen' onderzocht. Zes factoren blijken cruciaal te zijn voor het innovatievermogen van inlichtingen- en veiligheidsdiensten: visie en strategie, competentiebasis, leervermogen, creativiteit en het managen van ideeën, organisatiestructuur en tot slot cultuur.
De analyse laat ons zien dat geen van deze factoren dominant is in het begrijpen van het innovatievermogen van inlichtingen- en veiligheidsdiensten, maar dat zij op een complexe manier op elkaar inspelen. Bovendien botsen deze diensten en innovatie op verschillende vlakken met elkaar. Denk aan de spanning tussen geheimhouding en samenwerking met externe partijen, of aan het organiseren van innovatie naast de dagelijkse gang van zaken binnen de organisatie. En laten we niet vergeten dat inlichtingenproblemen soms op een heel andere manier moeten worden benaderd, zoals we hebben gezien bij de dreiging van de Chinese inlichtingendiensten.

Het onderzoek dat ik de komende jaren in het kader van mijn leerstoel *Intelligence in War & Conflict* ga doen zal zich met name richten op het innovatievermogen van inlichtingen- en veiligheidsdiensten. Concreet ga ik dieper graven naar de invloed en rol van de factoren die ik heb geïdentificeerd. Ik ben van plan dit te doen voor verschillende innovaties en in verschillende contexten. Het defensiedomein staat daarbij centraal. Ik wil vooral letten op een stevige methodologische basis, een multidisciplinaire aanpak en samenwerking tussen wetenschap en de diensten. Daarnaast richt ik me niet alleen op het niveau van de hele organisatie, maar ook op individueel- en teamniveau en wil ik naast losse gevallen ook vergelijkend onderzoek doen. En hoewel ik in mijn oratie alleen ben ingegaan op inlichtingen- en veiligheidsdiensten die met name op het politiek-strategisch niveau opereren, zal mijn onderzoek zich ook nadrukkelijk richten op het tactisch en operationeel niveau van militair optreden. Ik ben daarbij met name geïnteresseerd in inlichtingenorganisaties die werken in Navo, VN of EU-verband[64].

Dankwoord

Ik ben gekomen aan het einde van mijn oratie. Het feit dat ik hier sta heb ik aan velen van u te danken. Ik heb op het *Institute for Security and Global Affairs* (ISGA) en de Faculteit Militaire Wetenschappen (FMW) in Breda veel geweldige collega's, zowel militairen als burgers, met wie ik graag samenwerk. Ik wil al deze mensen bedanken voor hun bijdrage, en ook een aantal specifiek benoemen.

Om te beginnen de mensen die deze aanstelling mogelijk hebben gemaakt. Vanuit de Universiteit Leiden noem ik in het bijzonder Erwin Muller, Joachim Koops, Ernst Dijxhoorn en de huidige instituutsdirecteur Sanneke Kuipers. Van Bredase zijde zijn dit Patrick Oonincx en Paul Ducheine.

Tijdens mijn oratie aan de Nederlandse Defensie Academie in 2019 heb ik de mensen bedankt die een rol hebben gespeeld in mijn carrière en met wie ik nog steeds met veel plezier samenwerk. Ik zal het hier niet nogmaals herhalen, maar mijn dank aan jullie blijft groot. Ik maak daarbij één uitzondering en die is voor Myriame Bollen. Wat ontzettend fijn dat je hier vandaag kunt zijn.

Bij ISGA werk ik sinds twee jaar met veel plezier. Allereerst wil ik daarvoor de mensen van de onderzoeksgroep *Intelligence Studies* bedanken. Jullie zijn een stel zeer getalenteerde mensen met veel passie voor je werk. En daarnaast ook nog gewoon heel leuke mensen. Het is dan ook een voorrecht om met jullie samen te kunnen werken Damien, Simon, Tom, Ludo, Willemijn, Nikki, Giliam, Zakia, Eva, Yoeri, Christiaan en Lena. Vanuit de andere onderzoeksgroepen wil ik met name Ernst Dijxhoorn, Frans Osinga, Joachim Koops, Dennis Broeders, Vanessa Newby en Tom Buitelaar noemen en bedanken voor hun collegialiteit.
Ik heb het voorrecht om zowel aan de Nederlandse Defensie Academie als aan de Universiteit Leiden verbonden te zijn. Dit stelt me in staat deze werelden met elkaar te verbinden. Ik word er echt blij van als ik zie wat onze gezamenlijke activiteiten, onderzoeksprojecten en kennisuitwisseling opleveren. We gaan nog veel bereiken!
Na de zomer ga ik deeltijds aan de slag als vice-decaan onderzoek van de Faculteit Militaire Wetenschapen. Ik kijk er naar uit om samen met het Faculteitsbestuur en de collega's in Breda het militair onderzoek verder vorm te geven. In deze turbulente tijden is een stevige kennisbasis essentieel. Bovendien zal ik me inzetten om de samenwerking tussen de Nederlandse Defensie Academie en de Universiteit Leiden te versterken.

Verder wil ik collega's van verschillende universiteiten bedanken voor hun aanwezigheid. Ook de vertegenwoordigers van de MIVD, JISTARC en andere defensie-onderdelen verdienen een speciale vermelding. Veel van het onderwijs en onderzoek dat hier plaatsvindt, zal uiteindelijk ten goede komen aan jullie organisaties. Ik hecht veel waarde aan onze samenwerking en hoop deze in de toekomst te blijven versterken.

Rob, Stephen en Pepijn, dank voor jullie kritische blik bij de totstandkoming van deze oratie.

Ik wil veel vrienden bedanken voor jullie komst vandaag. Een aantal van jullie reageert weleens kritisch als ik weer eens voor onderzoek of een congres naar het buitenland moet. Ik krijg dan te horen dat het tenslotte op kosten van jullie belastinggeld is. Ik ga ervan uit dat jullie nu gerustgesteld zijn en hebben gezien welke inzichten jullie investeringen hebben opgeleverd.

Lieve familie en in het bijzonder mijn vader, zus, Anne, Juup en Noor. Ik sta hier vandaag met trots en blijdschap. Jullie zijn mijn anker, mijn kompas en mijn bron van inspiratie en innovatie. Samen hebben we nieuwe wegen bewandeld, grenzen verlegd en onontdekte paden betreden. Jullie steun en liefde hebben mijn leven verrijkt en mijn creativiteit aangewakkerd. Laten we blijven innoveren, samen lachen, huilen en groeien. Op naar nog vele avonturen!

Ik heb gezegd.

Noten

1. Claver, A., F. Van Nijnatten, and B.M.J. Pijpers. "'Zonder Inlichtingen Geen Veiligheid'". *Militaire Spectator,* Vol. 91, No. 9 (2022): 4-11. Quote op p. 11.
2. Enkele uitzonderingen zijn: Petrelli, N. "Analytical Innovation in Intelligence Systems: The US National Security Establishment and the Craft of 'Net Assessment'". *Intelligence and National Security,* Vol. 37, No. 1 (2022): 1-18; Wolfberg, A. and B.A. Pelley. "The Role of Innovation: Creating a Culture of Improvement". *American Intelligence Journal,* Vol. 26 (2009): 30-36; Zegart, A.B. "September 11 and the Adaptation Failure of Us Intelligence Agencies". *International Security,* Vol. 29, No. 4 (2005): 78-111.
3. Zie bijvoorbeeld: Kapantai, E., C. Androniki, C. Berberidis, and V. Peristeras. "A Systematic Literature Review on Disinformation: Toward a Unified Taxonomical Framework". *New Media & Society,* Vol. 23, No. 5 (2021): 1301-26.
4. Zie bijvoorbeeld: Robson Morrow, M.A. "Private Sector Intelligence: On the Long Path of Professionalization". *Intelligence and National Security,* Vol. 37, No. 3 (2022): 402-20.
5. Zie bijvoorbeeld Lim, K. "Big Data and Strategic Intelligence". *Intelligence and National Security,* Vol. 31, No. 4 (2016): 619-35.
6. Deze definitie is gebaseerd op de (militaire) innovatieliteratuur, zie: Sinterniklaas, R. *Military Innovation: Cutting the Gordian Knot*. Netherlands Defence Academy (Breda: Faculty of Military Sciences, 2018).
7. Voor een overzicht hoe technologie inlichtingen- en veiligheidsdiensten kan versterken, zie: Center for Strategic and International Studies (CSIS). "CSIS Launches Program on Intelligence, National Security, and Technology." (Washington: Center for Strategic & International Studies, 2021). Beschikbaar via: https://www.csis.org/news/csis-launches-program-intelligence-national-security-and-technology.
8. Spaceknow. *Lessons Learned from the Ukraine Invasion: The future of automation in satellite imagery analysis.* 19 september 2022. Beschikbaar via: https://spaceknow.com/blog/automation-in-satellite-imagery-analysis/
9. Pherson, R.H. and R.J. Heuer Jr. *Structured Analytic Techniques for Intelligence Analysis.* Third edition. (Washington DC: CQ Press, 2020).
10. Militaire Inlichtingen en Veiligheids Dienst (MIVD), *Openbaar jaarverslag 2023* (Den Haag: MIVD, 2024). Beschikbaar via: https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023
11. Lawson, B. and D. Samson. "Developing Innovation Capability in Organisations: A Dynamic Capabilities Approach". *International Journal of Innovation Management,* Vol. 5, No. 3 (2001): 377-400.
12. Strønen, F., T. Hoholm, K. Kværner, and L.N. Støme. "Dynamic Capabilities and Innovation Capabilities: The Case of the 'Innovation Clinic'". *Journal of Entrepreneurship, Management and Innovation (JEMI)*, Vol. 13, No. 1 (2017): 89-116
13. Gullmark, P. and T. Høyvarde Clausen. "In search of innovation capability and its sources in local government organizations: a critical interpretative synthesis of the literature." *International Public Management Journal,* Vol. 26, No. 2 (2023): 258-260.
14. Lawson and Samson, "Developing Innovation Capability in Organisations".
15. Ik baseer me hier met name op het baanbrekende werk van Lawson and Samson, "Developing Innovation Capability in Organisations". Zij identificeren het management van technologie als zevende factor. Vanwege de beperkte omvang van deze oratie en de overlap met de andere zes factoren heb ik het management van technologie niet expliciet meegenomen.
16. Lawson and Samson, "Developing Innovation Capability in Organisations".
17. Alderton, M. "CIA Deputy Director for Digital Innovation: 'Innovate or Perish'". *Trajectory: The*

official magazine of USGIF. Beschikbaar via: https://trajectorymagazine.com/cia-deputy-director-for-digital-innovation-innovate-or-perish/.

18. Blank, S. "The Red Queen Problem: Innovation in the Defense Department and Intelligence Community". *War on the Rocks* (October 17, 2017). Beschikbaar via: https://warontherocks.com/2017/10/the-red-queen-problem-innovation-in-the-defense-department-and-intelligence-community/.
19. Militaire Inlichtingen en Veiligheids Dienst (MIVD), *Openbaar jaarverslag 2022* (Den Haag: MIVD, 2023); Militaire Inlichtingen en Veiligheids Dienst (MIVD). *NLD DISS Innovation Agenda: Open innovation in a closed environment* (Den Haag: MIVD, 2022).
20. Zie bijvoorbeeld: Tuinier, P., T. Brocades Zaalberg, and S.J.H. Rietjens. "The Social Ties That Bind: Unraveling the Role of Trust in International Intelligence Cooperation". *International Journal of Intelligence and CounterIntelligence* 36, no. 2 (2023): 386-422.
21. Arcos, R., N.K. Drumhiller, and M. Phythian (eds). *The Academic-Practitioner Divide in Intelligence Studies* (London: Rowman & Littlefield, 2022).
22. Van Puyvelde, D. *Outsourcing Us Intelligence: Contractors and Government Accountability* (Edinburgh: Edinburgh University Press, 2022).
23. Gardner, F. "MI6 Must Adapt to New Technology to Survive, Says Spy Chief". *BBC News*, 30 november 2021. Beschikbaar via: https://www.bbc.com/news/uk-59470026.
24. Tuinier, Brocades Zaalberg, and Rietjens, "The Social Ties That Bind".
25. Claver, A. "Smart Intelligence Cooperation. NISA International Conference 2023". *Militaire Spectator,* Vol. 193, No. 1 (2024): 56-59.
26. Callum, R. "The Case for Cultural Diversity in the Intelligence Community". *International Journal of Intelligence and CounterIntelligence,* Vol. 14, No. 1 (2001): 25-48.
27. Syed, M. *Rebel Ideas: The Power of Diverse Thinking* (London: John Murray Publishers, 2020).
28. Zie: https://jscu.summerschool.sh
29. Kesting, P., J.P. Ulhøi, L.J. Song and H. Niu. "The impact of leadership styles on innovation management - a review and a synthesis". *Journal of Innovation Management,* Vol. 3, No. 4 (2015): 22-41.
30. Zie: https://www.aivd.nl/actueel/nieuws/2020/08/31/aivd-herdenkt-arthur-docters-van-leeuwen
31. Romme, G.L., and A. Van Witteloostuijn. "Circular Organizing and Triple Loop Learning". *Journal of Organizational Change Management,* Vol. 12, No. 5 (1999): 439-54.
32. Treverton, G. "Risks and riddles: The Soviet Union was a puzzle. Al Qaeda is a mystery. Why we need to know the difference". In: *Smithsonian Magazine*, Juni 2007. Beschikbaar via: https://www.smithsonianmag.com/history/risks-and-riddles-154744750/.
33. Eftimiades, N. "On the Question of Chinese Espionage". *Brown Journal of World Affairs,* Vol. 26, No. 1 (2019): 125-142.
34. Rijksdienst voor Ondernemend Nederland. *China's Pursuit of Overseas Brains: The 1,000 Talents Policy.* 2017. Beschikbaar via: https://www.rvo.nl/sites/default/files/2017/01/1000-Talents-Policy-Article.pdf
35. Zie: https://liveuamap.com
36. Zie o.a. Gibson, S.D. "Open Source Intelligence." In: Dover, R., M.S. Goodman and C. Hillebrand (eds.). *Routledge Companion to Intelligence Studies.* (London: Routledge, 2014): 123-131.
37. Alderton, "CIA Deputy Director for Digital Innovation: 'Innovate or Perish'". Deze observatie reflecteert ook de OSINT-strategie van de Amerikaanse Director of National Intelligence (DNI) die in maart van dit jaar is uitgegeven. De titel van deze strategie is veelzeggend: "The INT of First Resort: Unlocking the value of OSINT". Director of National Intelligence (DNI) (2024). *The IC OSINT Strategy 2024-2026: The INT of First Resort. Unlocking the*

Value of OSINT. Beschikbaar via: https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
38. Agrell, W. "When everything is intelligence – nothing is intelligence". In: *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, Vol. 1, No. 4 (2002): 2-6.
39. Zie: https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20090520_speech.pdf
40. Lovelace, R. "CIA Goes Back to School to Collaborate on Spy Tech Research". *The Washington Times*, March 10, 2022, Beschikbaar via: https://www.washingtontimes.com/news/2022/mar/10/cia-goes-back-school-collaborate-spy-tech-research/.
41. Rogers, E.M. *Diffusions of innovations.* Fifth edition (New York: Free Press, 2003).
42. Bob, Y.J. "Shin Bet Reveals, for the First Time, Its Tech 'Garage'". *The Jerusalem Post*, March 2, 2022. Beschikbaar via: https://www.jpost.com/breaking-news/article-699022.
43. Perry-Smith, J. and P.V. Mannucci. "Social Networks, Creativity, and Entrepreneurship". In: C.E. Shalley, M.A. Huitt and J. Zhou (eds.), *The Oxford Handbook of Creativity, Innovation, and Entrepreneurship* (Oxford: Oxford University Press, 2015): 205-224.
44. Coulthart, S.. "From Laboratory to the WMD Commission: How Academic Research Influences Intelligence Agencies". *Intelligence and National Security,* Vol. 34, No. 6 (2019): 818-32.
45. Blank, "The Red Queen Problem".
46. Marchio, J.D. "Fostering Creativity in the IC: Insights from Four Decades Ago". *Studies in Intelligence,* Vol. 65, No. 4 (2021): 19-28.
47. Burgelman, R.A. *Strategic Management of Technology and Innovation* (Irwin, IL: Homewood, 1988).
48. Office of the Director of National Intelligence, Remarks by the Director of National Intelligence Mr. Dennis Blair. Beschikbaar via: https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20100222_speech.pdf
49. Agger, Annika, and Eva Sørensen. "Managing Collaborative Innovation in Public Bureaucracies". *Planning Theory,* Vol. 17, No. 1 (2018): 53-73.
50. O'Reilly, C.A., III, and M.L. Tushman. "Organizational ambidexterity: Past, present, and future". *Academy of Management Perspectives,* Vol. 27, No. 4 (2013): 324–338.
51. O'Reilly, C.A., III and M.L. Tushman "Organizational ambidexterity: Past, present, and future"; Heeren-Bogers, J., R. Moelker, E. Kleinreesink, J. van der Meulen, J.M.M.L. Soeters, and R. Beeres (eds.). *The Yin-Yang Military: Ambidextrous Perspectives on Change in Military Organizations* (Cham: Springer, 2020).
52. O'Reilly, C. A., III and M.L. Tushman. "Ambidexterity as a dynamic capability: Resolving the innovator's dilemma". *Research in Organizational Behavior,* Vol. 28 (2008): 185–206.
53. Tushman, M.L. and E. Romanelli. "Organizational evolution: A metamorphosis and model of convergence and reorientation". *Research in organizational behavior,* Vol. 7 (1985): 171–222; Gersick, C.J. "Revolutionary change theories: A multilevel exploration of the punctuated equilibrium". *Academy of Management Review*, Vol. 16, No. 1 (1991): 10–36; Waard, E.J. de, and T. Bijlsma. "African Winds: Versatile Value Creation in the Military". In: Heeren-Bogers, J., R. Moelker, E. Kleinreesink, J. van der Meulen, J.M.M.L. Soeters, and R. Beeres (eds.). *The Yin-Yang Military: Ambidextrous Perspectives on Change in Military Organizations* (Cham: Springer, 2020): 37-50.
54. Zegart. "September 11 and the Adaptation Failure of U.S. Intelligence Agencies".
55. Shields, P.M. and D.S. Travis. "Resolving Contradictions in Military Operations via Ambidexterity". In: Heeren-Bogers, J., R. Moelker, E. Kleinreesink, J. van der Meulen, J.M.M.L. Soeters, and R. Beeres (eds.). *The Yin-Yang Military: Ambidextrous Perspectives on Change in Military Organizations* (Cham: Springer, 2020): 3-17.

56. O'Reilly and Tushman. "Organizational ambidexterity: Past, present, and future".
57. Uotila, J., M. Maula, T. Keil, and S.A. Zhara. "Exploration, exploitation and firm performance: An analysis of S&P 500 corporations". *Strategic Management Journal*, Vol 30, No. 2 (2009), p. 221-231.
58. Lawson and Samson, "Developing Innovation Capability in Organisations".
59. CSIS Technology and Intelligence Task Force, *Maintaining the Intelligence Edge*, ix.
60. Pardo del Val, Manuela, and Clara Martinez Fuentes. "Resistance to Change: A Literature Review and Empirical Study". *Management decision,* Vol. 41, No. 2 (2003): 148-55.
61. Zie bijvoorbeeld: Aldrich, R.J. and C.R. Moran. "'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy". *Political Studies*, Vol. 67, No. 2 (2019): 291-306; Aldrich, R.J., and D. Richterova. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy". *West European Politics* Vol. 41, No. 4 (2018): 1003-24; Moran, C. *Classified: Secrecy and the State in Modern Britain.* (Cambridge: Cambridge University Press, 2013).
62. Braat, E. "Self-Reinforcing Secrecy: Cultures of Secrecy within Intelligence Agencies". In: Mokrosinska, D. (ed.). *Transparency and Secrecy in European Democracies* (London and New York, NY: Routledge, 2020): 118-34.
63. Merton, R.K. "Bureaucratic Structure and Personality". *Social Forces,* Vol. 18 (1940): 560-68. Quote o p. 560.
64. Zia o.a. Waard, E.J. de, S.J.H. Rietjens, A.G.L. Romme, P.C. van Fenema. "Learning in complex public systems: The case of MINUSMA's intelligence organization". *Public Management Review*, Vol. 25, No. 6 (2023): 1039-1058; Rietjens, S.J.H. "NATO's Struggle for Intelligence in Afghanistan." *Armed Forces & Society,* Vol. 49, No. 4 (2023): 1001-1012.

Prof.dr.ir. Sebastiaan J.H. Rietjens

Sebastiaan (Bas) Rietjens is hoogleraar Inlichtingen & Veiligheid aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie en tevens bijzonder hoogleraar *Intelligence in War & Conflict* aan het *Institute of Security and Global Affairs* van de Universiteit Leiden. Het onderwijs en onderzoek van Bas richt zich op inlichtingen in het militaire domein en dan met name op militaire operaties, hybride dreigingen, samenwerking en innovatie. Hij vindt het daarbij van groot belang om de brug te slaan tussen wetenschap en praktijk. Bas heeft uitgebreid veldwerk gedaan tijdens militaire oefeningen en operaties waaronder Afghanistan (ISAF), Mali (MINUSMA), Griekenland (FRONTEX), Polen en de Baltische Staten (NATO) en meer dan 130 wetenschappelijke publicaties op zijn naam staan. Hij is redactielid van de tijdschriften *Armed Forces & Society* en *International Journal of Intelligence & Counterintelligence*, bestuurslid van de *Netherlands Intelligence Studies Association* (NISA) en redacteur van verschillende bundels waaronder het *Routledge Handbook of Research Methods in Military Studies* (Routledge, 2014) en *Reflections on the Russia-Ukraine War* (Leiden University Press, 2024). Vanaf de zomer 2024 zal hij tevens in deeltijd de functie van vice-decaan onderzoek aan de Faculteit Militaire Wetenschappen gaan bekleden. Bas is te bereiken op: sjh.rietjens.01@mindef.nl.

Universiteit Leiden