



RISICO- EN DREIGINGSBEELD

Hoger Onderwijs 2024

MANAGEMENTSAMENVATTING

Achtergrond

Het hoger onderwijs wordt geconfronteerd met een breed scala aan risico's en dreigingen die continu in beweging zijn en om constante aandacht voor het aanpassen en versterken van integraal veiligheidsbeleid vragen. Het voorliggende Risico- en Dreigingsbeeld Hoger Onderwijs 2024 beoogt hoger onderwijsinstellingen een kader te bieden bij de afweging welke risico's en dreigingen voor de eigen instellingen het meest relevant zijn of in de nabije toekomst relevant zullen worden. Het biedt daarmee een instrument om prioriteiten te kunnen stellen in het eigen veiligheids- en organisatiebeleid. Iedere instelling is immers anders. Het Risico- en Dreigingsbeeld Hoger Onderwijs 2024 is geschreven in opdracht van het Platform Integrale Veiligheid Hoger Onderwijs.

Meest impactvolle trends

Het risico- en dreigingslandschap voor hoger onderwijsinstellingen wordt steeds complexer en uitdagender door veranderende sociale dynamieken, de snelle vooruitgang van technologieën en toenemende geopolitieke spanningen. De vijf meest impactvolle ontwikkelingen van de afgelopen drie jaar, die naar verwachting ook in de komende jaren risico's en dreigingen voor het hoger onderwijs met zich mee zullen brengen, zijn:

- Een toename in internationale geopolitieke (economische en technologische) competitie, conflicten en crisis, met een bijbehorende toename in ongewenste beïnvloeding door statelijke actoren.

- Groeiende maatschappelijke uitdagingen, waaronder geestelijke gezondheidszorg en innesteling van criminele organisaties in de maatschappij.
- Toename van activisme, zorgwekkend gedrag en radicalisering.
- Het vergroten van bestaande risico's en dreigingen door technologische ontwikkelingen, waarbij enkele ontwikkelingen mogelijk op zichzelf een risico kunnen vormen.
- Beknotting van academische vrijheid, wat op de lange termijn de kwaliteit van onderwijs en onderzoek kan aantasten en wat mogelijk ook grote gevolgen kan hebben voor de concurrentiepositie van HO-instellingen.

Scenario's

Drie toekomstverkenningen (scenario's) maken zichtbaar hoe risico's en dreigingen voor het hoger onderwijs zich mogelijk de komende jaren kunnen gaan manifesteren.

- In het scenario "Een handvol handige hackers" nemen een klein aantal *hacktivisten* het heft in eigen handen en zorgen er met verschillende (digitale) acties uiteindelijk voor dat het college van bestuur zich genoodzaakt ziet om af te treden. Het illustreert de grote impact die activistische acties kunnen hebben op sociale, fysieke én informatieveiligheid, wat de noodzaak tot investeren in (cyber)weerbaarheid onderstreept.

- Het scenario "Waar een wil is, is een (om)weg" laat zien hoe kwaadwillende statelijke actoren nieuwe (digitale) wegen zoeken om alsnog hun doelen te bereiken – het zogenaamde "waterbedeffect". Het is daarom belangrijk om altijd het adagium *assume breach* voor ogen te hebben en maatregelen te nemen die niet alleen de *kans* op inbreuk beperken maar ook de *impact* ervan verkleinen.
- In het scenario "Soeverein in eigen brein" zorgt een combinatie van ontwikkelingen voor een toename in alternatieve vormen van onderwijs, hetgeen op de langere termijn de bestaanszekerheid van Nederlandse HO-instellingen bedreigt. Het scenario benadrukt het belang van voortdurende technologische en maatschappelijke innovatie van het hoger onderwijs, maar ook hoe risico's kunnen worden omgezet in kansen.

Handvatten

Ondanks de grote verschillen tussen de HO-instellingen voor wie dit Risico- en Dreigingsbeeld Hoger Onderwijs 2024 geschreven is, zijn er op basis van dit document een aantal brede handvatten te formuleren:

- Een **integrale aanpak van veiligheid** en een **goed ontwikkeld risicomanagement** zijn essentieel om alle uitdagingen het hoofd te bieden.
- De onzekerheid rondom de impact van nieuwe ontwikkelingen noopt tot een **toekomstgerichte en wendbare aanpak**.

- Het adagium **assume breach** is belangrijk om niet enkel de kans op een ongewenste gebeurtenis, maar ook de potentiële impact ervan te verkleinen.
- Een aantal risico's en dreigingen zijn dermate urgent dat **actie op de korte termijn** geboden is. Vaak vragen uitdagingen ook om beleid met een lange adem.
- Kijkend naar de toekomst zijn het **vergroten van cyberweerbaarheid** en het **versterken van risico-management** belangrijke speerpunten van beleid. Voor deze maatregelen zal meer **mankracht** en **expertise** nodig zijn.
- Tot slot is **flexibiliteit** geboden om aan de grote veranderingen in de maatschappij en het hoger onderwijslandschap het hoofd te kunnen bieden. Zo zullen hoger onderwijsinstellingen consequent moeten innoveren, zowel op technologisch als maatschappelijk gebied.

Alleen door gezamenlijke inspanningen en een voortdurende toewijding aan veiligheid en veerkracht kunnen hoger onderwijsinstellingen een veilige en stimulerende leeromgeving bieden voor studenten, wetenschappers, docenten en medewerkers – zowel nu als in de (verre) toekomst.



INHOUDSOPGAVE

| | | | |
|----------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Managementsamenvatting | 4 | Toenemende radicalisering en zorgwekkend gedrag vormen een dreiging voor de veiligheid van HO-instellingen | 27 |
| 1. INLEIDING | 8 | Technologische ontwikkelingen brengen nieuwe risico's en dreigingen met zich mee en kunnen bestaande risico's en dreigingen vergroten. | 28 |
| 2. OVERZICHT RISICO'S EN DREIGINGEN PER THEMA | 12 | Toenemende beknotting van academische vrijheid ondergraaft een fundamentele voorwaarde voor hoogwaardig onderwijs en onderzoek | 29 |
| Integriteit | 12 | 4. RISICO'S EN DREIGINGEN VOOR HET HOGER ONDERWIJS: DRIE VOORSTELBARE TOEKOMSTEN | 32 |
| Arbo en milieu | 13 | Scenario 1: Een handvol handige hackers | 32 |
| Sociale veiligheid | 14 | Scenario 2: Waar een wil is, is een (om)weg | 35 |
| Zorgwekkend gedrag en radicalisering | 15 | Scenario 3: Soeverein in eigen brein | 38 |
| Gebouwveiligheid, beveiliging en BHV | 16 | 5. CONCLUSIES | 41 |
| Internationalisering | 17 | Bijlage 1. Methodologische verantwoording | 42 |
| Cyberveiligheid | 18 | Bijlage 2. Bibliografie | 47 |
| Privacy | 19 | | |
| Kennisveiligheid en ongewenste beïnvloeding | 20 | | |
| 3. HET RISICO- EN DREIGINGSLANDSCHAP: VIJF BELANGRIJKE (TOEKOMSTIGE) TRENDS | 24 | | |
| Geopolitieke competitie, internationale conflicten en crises hebben steeds meer impact op het hoger onderwijs | 24 | | |
| Maatschappelijke problemen leiden tot steeds meer druk op HO-instellingen, wat de rol en positie van het hoger onderwijs aantast | 25 | | |



INLEIDING

1 INLEIDING

Het hoger onderwijs is een cruciale pijler van onze maatschappij waar kennis wordt gedeeld, innovatie wordt gestimuleerd en waar de leiders van morgen worden gevormd. Het waarborgen van deze taken is echter geen vanzelfsprekendheid. Hoger onderwijsinstellingen worden geconfronteerd met een breed scala aan risico's en dreigingen. Vaak zijn deze onlosmakelijk verbonden met de maatschappelijke uitdagingen waar Nederland voor staat.

Nieuwe ontwikkelingen vragen om constante aandacht voor het aanpassen en versterken van integraal veiligheidsbeleid om zo een veilig leer- en werkklimaat en bedrijfscontinuïteit te garanderen, iets waartoe hoger onderwijsinstellingen zich via een intentieverklaring via hun koepels hebben gecommitteerd (IVHO, 2018). Dit Risico- en Dreigingsbeeld Hoger Onderwijs 2024 beoogt daaraan bij te dragen door hoger onderwijsinstellingen een kader te bieden voor de afweging welke risico's en dreigingen voor de eigen instellingen het meest relevant zijn. Het is daarmee een instrument voor de instellingen om prioriteiten te kunnen stellen in het eigen veiligheids- en organisatiebeleid. Iedere instelling is immers anders in omvang, organisatie, doelstellingen, studentenpopulatie, ligging en activiteiten.

Het Risico- en Dreigingsbeeld Hoger Onderwijs 2024 is geschreven in opdracht van het Platform Integrale Veiligheid Hoger onderwijs (hierna: Platform IV-HO). Voorgaande edities verschenen in 2018 en 2021 (Van

der Varst et. al., 2018; IVHO & COT, 2021). Waar het gaat om cyberdreigingen bouwt het voort op het door SURF gepubliceerde Cyberdreigingsbeeld 2023. Daarnaast put het voor relevante thema's uit verschillende publicaties van de inlichtingen- en veiligheidsdiensten, het *Dreigingsbeeld Statelijke Actoren* (AIVD, MIVD & NCTV, 2022) en meerdere publicaties van het *Dreigingsbeeld Terrorisme Nederland* van de NCTV.

De opdracht van Platform IV-HO aan de onderzoekers was om in deze editie de aandacht te richten op een verkenning van toekomstige risico's en dreigingen. In dit Risico- en Dreigingsbeeld Hoger Onderwijs ligt de nadruk dan ook op de bespreking van vijf actuele trends en drie scenario's waarin belangrijke toekomstige risico's en dreigingen een plaats hebben gekregen. Binnen de trends en scenario's komt de verwevenheid van de verschillende maatschappelijke ontwikkelingen en de risico's en dreigingen die zij met zich meebrengen duidelijk naar voren. De vijf beschreven trends richten zich op de volgende terreinen: (1) geopolitieke competitie, internationale conflicten en crises, (2) de druk om maatschappelijke taken op te pakken, (3) radicalisering en zorgwekkend gedrag, (4) opkomende technologieën en (5) beknotting academische vrijheid. De scenario's zijn onder meer gericht op voorstelbare toekomstige vormen van activisme, mogelijke waterbedeften van spionage en (heimelijke) beïnvloeding, en de hoge mate van flexibiliteit die snelle technologische ontwikkelingen mogelijk van HO-instellingen vereisen.

Daaraan voorafgaand biedt het Risico- en Dreigingsbeeld Hoger Onderwijs 2024 een beknopt overzicht van actuele risico's en dreigingen en ontwikkelingen daarbinnen sinds de vorige editie in 2021. Dit wordt gedaan aan de hand van drie domeinen en negen thema's, aangereikt door het Platform IV-HO, waarbinnen risico's en dreigingen zich kunnen manifesteren. De drie domeinen zijn sociale veiligheid, informatieveiligheid en fysieke veiligheid. De thema's zijn: integriteit, arbo en milieu, sociale veiligheid, zorgwekkend gedrag en radicalisering, gebouwveiligheid, beveiliging en BHV, internationalisering, cyberveiligheid, kennisveiligheid en ongewenste beïnvloeding en privacy. Deze domeinen en thema's, die onderling (deels) overlappen, worden gedefinieerd in hoofdstuk 2.

Totstandkoming en werkwijze

Om zo breed mogelijk inzichten te vergaren in de mogelijke risico's en dreigingen die zich in de komende vijf jaar kunnen uiten binnen HO-instellingen, is voor dit onderzoek gekozen voor een gevarieerd palet aan methodes om input te verzamelen en deze vervolgens uit te werken. Daarbij is gebruik gemaakt van open bronnenonderzoek, *strategic foresight* methodieken – waaronder *horizonscanning* en *scenario-building* –, interviews met experts en meerdere dialoogtafels met stakeholders uit een diverse groep hoger onderwijsinstellingen en gelieerde organisaties. Zie bijlage 1 voor een gedetailleerde methodologische verantwoording.

Doelgroep

Dit document is bestemd voor een diverse groep stakeholders in het hoger onderwijs, waaronder bestuurders, integrale veiligheidsmedewerkers en beleidsmedewerkers binnen deze instellingen. Tegelijkertijd kan dit document gelezen en gebruikt worden door koepelorganisaties, zoals de Vereniging Hogescholen (VH) en Universiteiten van Nederland (UNL), alsook verschillende overheidsinstanties.

Gezien de omvang van de doelgroep is gekozen om een beknopt overzicht van alle risico's en dreigingen toe te voegen (hoofdstuk 2), ook al is dit voor de medewerkers die hier dagelijks mee te maken hebben mogelijk niet essentieel. Het biedt echter wel een schriftelijke onderbouwing van de praktijk, wat kan worden gebruikt als referentiepunt.

Leeswijzer

Hoofdstuk 2 biedt een overzicht van ontwikkelingen rondom actuele risico's en dreigingen op de negen bovengenoemde thema's. In hoofdstuk 3 worden vijf voor het hoger onderwijs belangrijke trends en hun actuele en toekomstige impact op risico's en dreigingen voor het hoger onderwijs besproken. Hoofdstuk 4 presenteert drie voorstelbare toekomstige scenario's. Hoofdstuk 5 bevat conclusies en biedt enkele handelingsperspectieven.



Risico's en Dreigingen.

Beiden begrippen gaan over een gebeurtenis die in de toekomst kan plaatsvinden. Het verschil is dat er bij een *dreiging* aantoonbare informatie beschikbaar is dat er iets staat te gebeuren, terwijl het bij een *risico* gaat om de kans dat een gewenste of ongewenste gebeurtenis zich zal manifesteren in combinatie met de impact van zo'n gebeurtenis.



**HO-INSTELLINGEN MOETEN VAAK
NOODGEDWONGEN, STEEDS MEER
ADDITIONELE TAKEN OP ZICH NEMEN
WAARVOOR ZIJ IN MINDERE MATE OF
NIET ZIJN INGERICHT EN WAARVOOR
ZIJ WEINIG TOT GEEN CAPACITEIT
HEBBEN.**



OVERZICHT RISICO'S EN DREIGINGEN PER THEMA

2 OVERZICHT RISICO'S EN DREIGINGEN PER THEMA

Dit hoofdstuk biedt een kort overzicht van actuele risico's en dreigingen op de thema's die onderdeel zijn van integraal veiligheidsbeleid aan hoger onderwijsinstellingen. Zij vallen binnen één of meerdere van de domeinen sociale veiligheid, fysieke veiligheid en informatieveiligheid (figuur 1).¹

Definities van de domeinen

Sociale veiligheid is de mate waarin mensen beschermd zijn en zich beschermd voelen tegen persoonlijk leed veroorzaakt door anderen.

Fysieke Veiligheid is de mate waarin mensen beschermd zijn en zich beschermd voelen tegen persoonlijk leed van niet-menselijke oorsprong.

Informatieveiligheid is de mate waarin onderwijs, onderzoek, kennis en digitale systemen beschermd zijn tegen ongewenste beïnvloeding en misbruik.

De meeste van deze thema's komen ook (expliciet of impliciet) aan de orde in de beschrijving van de brede veiligheidstrends die het hoger onderwijs raken (Hoofdstuk 3) en in de scenario's (Hoofdstuk 4). De drie hoofdstukken tezamen illustreren daarbij zowel

de onderlinge verwevenheid van de thema's, als de verwevenheid van de thema's met maatschappelijke ontwikkelingen.



FIGUUR 1. GEVISUALISEERDE OVERLAP VAN DOMEINEN EN THEMA'S.

Integriteit

Integriteit behelst het streven naar eerlijkheid, betrouwbaarheid, oprechtheid en transparantie van medewerkers en studenten individueel en de instelling als geheel. Wetten, regels en codes helpen normen te stellen die moeten worden nageleefd (IVHO & COT, 2021).

Ontwikkelingen sinds 2021

- In de afgelopen jaren is er aandacht besteed aan versterking van wetenschappelijke integriteit met bijvoorbeeld de publicatie van een 'Landelijk Model Klachtenregeling Wetenschappelijke Integriteit' (UNL, 2023). Ook is transparantie met betrekking tot nevenwerkzaamheden bevorderd door de invoering van een aangescherpte 'Sectorale regeling nevenwerkzaamheden Nederlandse universiteiten 2024'. Sinds kort publiceren alle universiteiten een publiek toegankelijk overzicht van de nevenwerkzaamheden van hun hoogleraren (UNL, 2024b).
- Statistieken laten een afname in klachten rondom wetenschappelijke integriteit zien op universiteiten, van 22 klachten in 2021 tot 16 in 2023 (LOWI, z.d.).²
- UNL ontwikkelt momenteel handvatten en beleid zodat AI en taalmodellen (LLMs) op een verantwoorde manier, in lijn met o.a. de code wetenschappelijk

¹ De domeinen zijn opgesteld en gedefinieerd door Platform IV-HO.

² Er zijn geen gegevens gepubliceerd over integriteitsklachten op hogescholen.

integriteit, gebruikt kunnen worden door studenten en onderzoekers.

Actuele risico's en dreigingen

- Fabriceren, vervalsen, plagiaat, fraude, verduistering, datalekken, ongewenste omgangsvormen door studenten en medewerkers, belangenverstrengeling, financiële afhankelijkheid, misbruik bevoegdheid door medewerkers en schending informatieplicht door medewerkers en instellingen.
- Misbruik door criminelen van infrastructuur van het hoger onderwijs en onderzoeksoopdrachten voor zaken als fraude, verduistering, witwassen, het moedwillig beschadigen van (de reputatie) van een wetenschapper of instelling.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Toename zelfcensuur door toename polarisering van het maatschappelijk debat en politisering van de wetenschap.

➤ **Impact:** aantasting kwaliteit onderwijs en onderzoek; imago-schade kennisinstelling; financiële en/of juridische gevolgen.

Schending integriteit in de praktijk

- Zes Zuidaskantoren en de belastingdienst beslissen mee over de aanstelling van docenten en de inhoud van het onderwijs. UVA doet momenteel onderzoek naar mogelijke integriteitsschending (afronding in het voorjaar van 2024) en heeft de minister van OCW toegezegd de uitkomsten van de evaluatie openbaar te maken (FTM, 2023).
- Twee Nederlandse wetenschappers zijn ingegaan op lucratieve aanbiedingen van Saoedische universiteiten om een dienstverband aan te gaan, die de betreffende universiteiten zou helpen stijgen op internationale ranglijsten (NOS, 2023b).

Arbo en milieu

Arbo en milieu. Arbo behelst het bevorderen van gezonde arbeids- en studeeromstandigheden en het voorkomen van veiligheidsrisico's voor medewerkers, studenten en derden. Milieu is nauw verwant aan Arbo en betreft de zorg voor onze leefomgeving. Verwaarlozing van die omgeving heeft effect op mensen, planten en dieren en beïnvloedt daarmee de gezonde en veilige werk- en leeromgeving (IVHO & COT, 2021).

Ontwikkelingen sinds 2021

- De werkdruk in het hoger onderwijs is hoog. In 2022 werd gerapporteerd dat 77% van het voltijd werkende wetenschappelijke personeel bij universiteiten veel of zeer veel werkdruk ervoer en dat 35-45% aangaf last van uitputtingsverschijnselen te hebben (BZK, OCW & CBS, 2022). Onderzoek bij het HBO geeft eenzelfde beeld: HBO-docenten draaien per week 30% meer uren dan in hun contract vermeld staat. De coronacrisis en de bijbehorende digitalisering van het onderwijs hebben de werkdruk de afgelopen jaren extra aangescherpt (VH, 2024).
- Sinds de coronapandemie wordt er meer thuisgewerkt: werknemers werkten in 2023 gemiddeld 6,8 uur per week vanuit huis, terwijl dit eind 2019 nog gemiddeld 2,6 uur was (TNO, 2023).
- Het percentage studenten dat aangeeft veel of heel veel stress te ervaren door hun studie is weliswaar enigszins afgenomen in de laatste drie jaar, maar in 2023 had nog altijd 44% van de studenten last van angst- en depressieklachten en ervaarde 56% (heel) veel stress (RIVM, 2023).
- Het Ministerie van OCW heeft circa €13 miljoen beschikbaar gesteld om te onderzoeken hoe onderwijsinstellingen onderwijs slimmer kunnen inrichten en het aantal weken met onderwijs en/of tentamens kunnen terugbrengen (OCW, 2023a). Het verminderen van werkdruk is ook meegenomen in de nieuwe CAO van het HBO. Tevens ligt er een voorstel om het bindend studieadvies aan te passen.

Actuele risico's en dreigingen

- Voor medewerkers: Hoge werkdruk en fysieke problemen door een ongeschikte werkplek bij thuiswerken, en stress door een (te) hoge werkdruk.
- Voor studenten: Aantasting mentale gezondheid door stress (RIVM, 2023).

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Druk op hogescholen en universiteiten om te voorzien in mentale gezondheidszorg door lange wachtlijsten in de geestelijke gezondheidszorg van gemeenten.
- Natuurgeweld met grote impact door klimaatverandering (NIPV, 2022).
- Onverwachte effecten van de energietransitie door nieuwe, minder bekende, infrastructuur en (gevaarlijke) producten (NIPV, 2022)

➤ **Impact:** Dreiging voor fysieke veiligheid, toename ziekteverzuim en aantasting kwaliteit van onderwijs en onderzoek.

Risico's arbo en milieu in de praktijk

- De invoering van de basisbeurs in 2023 helpt studenten rondkomen maar het bedrag is niet kostendekkend waardoor lenen en/of een bijbaan meestal nodig blijft (Kammer & Stefanovski, 2023).

Sociale veiligheid

Sociale veiligheid is de mate waarin medewerkers en studenten zich beschermd voelen en daadwerkelijk beschermd zijn tegen persoonlijk leed veroorzaakt door menselijk gedrag en/of handelen. Het betreft onder meer de bescherming tegen uitsluiting, pesten, (seksuele) intimidatie, discriminatie en racisme.

Ontwikkelingen sinds 2021

- Een groot aantal studenten aan hogescholen en universiteiten heeft seksueel grensoverschrijdend gedrag (SGG) meegemaakt. Eén onderzoek wijst uit dat het aantal meldingen aan Nederlandse universiteiten steeg van 141 meldingen in 2019, naar 300 meldingen in 2022 (Hamer, 2024).³

³ Er zijn geen gegevens gepubliceerd over de hoeveelheid meldingen op hogescholen.

- Er bestaat mogelijk een discrepantie tussen het aantal gevallen dat door onderzoekers wordt gerapporteerd en het aantal meldingen dat daadwerkelijk wordt gemaakt wegens gebrek aan vertrouwen in de klachtenprocedure (Inspectie van het Onderwijs, 2022; Hamer, 2024).
- Ook het aantal meldingen van niet-seksueel grensoverschrijdend gedrag is de afgelopen tijd gestegen. Hierbij spelen groeiende geopolitieke spanningen, politisering van de wetenschap en polarisering in maatschappelijk debat een belangrijke rol. Zo zijn het aantal meldingen van antisemitische incidenten is sinds de Gaza-oorlog verveelvoudigd (Giele, 2023) en zijn meldingen van discriminatie, belaging en mishandelingen van transgender personen in 2023 verdubbeld ten opzichte van het jaar ervoor (NCTV, 2023c).
- Door een gebrek aan samenhang tussen de verschillende rapportages en de verschillende manieren waarop incidenten worden gemeten is er een onduidelijk beeld ontstaan over sociale veiligheid op HO-instellingen.
- Het ministerie van OCW heeft in juni 2023 aangekondigd een integrale aanpak voor bevordering van een veilige werk- en leeromgeving te ontwikkelen (Dijkgraaf, 2023b). Ook nemen steeds meer hogescholen en universiteiten het thema sociale veiligheid op in hun curricula (NOS, 2023a). Echter zijn deze maatregelen op diverse onderdelen, waaronder seksueel overschrijdend gedrag, mogelijk niet afdoende om

de benodigde cultuurverandering teweeg te brengen (NOS, 2024b).

Actuele risico's en dreigingen

- Instandhouding van gevoelens van sociale onveiligheid ten gevolge van discriminatie, pestgedrag, (verbale) agressie, geweld en (seksueel) grensoverschrijdend gedrag.
- Gebrek aan vertrouwen in de klachtenprocedure en daarmee mogelijk een gebrek aan bereidheid bij staf en studenten om onveilige situaties te melden. Dit kan in sommige gevallen leiden tot zelfcensuur.
- Onvoldoende inzicht van bestuurders in de problematiek.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Toename zelfcensuur door toename polarisering van het maatschappelijk debat en politisering van de wetenschap.

➤ **Impact:** Aantasting kwaliteit van onderwijs en onderzoek, onder andere door zelfcensuur (Technopolis, 2022), leed en psychische klachten ten gevolge van sociale onveiligheid, imagoschade kennisinstelling, juridische gevolgen.

Inbreuk op sociale veiligheid in de praktijk

- In 2023 schetst De Gelderlander, na ruim dertig gesprekken met meer dan twintig vrouwen werkzaam bij de Radbouduniversiteit, een beeld van een ingesleten giftige vrouwenonvriendelijke cultuur op diverse plekken binnen de universiteit (Wassenaar & Winters, 2023).
- Veel hoger onderwijsinstellingen blijven anti-spiek tentamensoftware, die volgens het College voor de Rechten van de Mens mogelijk studenten met een zwarte huidskleur discrimineert, gebruiken (Hulsen, 2024; CRM, 2023).

Zorgwekkend gedrag en radicalisering

Zorgwekkend gedrag en radicalisering zijn de uitingen en het proces waarbij de gedachten en gedragingen van een persoon of groep (in toenemende mate) afwijken van, of zelfs haaks staan op, de democratische rechtsorde (Nederlands Jeugdinstituut, z.d.; AIVD, 2024). Dit uit zich onder andere in signalen of concrete gedragingen die wijzen op de bereidheid om te dreigen met het gebruik van geweld, of het daadwerkelijk gebruiken van geweld. Deze bereidheid kan

voortkomen uit religieuze of ideologische overtuigingen (terrorisme), geestelijke problematiek of een combinatie daarvan (IVHO & COT, 2021).⁴

Ontwikkelingen sinds 2021

- Geopolitieke spanningen hebben vaker een polariserend effect op delen van de samenleving.
- In december 2023 is het dreigingsniveau terrorisme door de NCTV verhoogd van 3 naar 4. Dit betekent dat de kans op een terroristische aanslag reëel wordt geacht.
- De aard van terroristische dreigingen is veelzijdiger en diffuser geworden: radicalisering vindt steeds meer online en individueel plaats, wat het fenomeen onvoorspelbaar maakt.
- Terroristische dreiging vanuit de extremistische islamitische hoek is toegenomen door koranschendingen, de Gaza-oorlog en polarisatie in Europa. Er is een toename in signalen dat jihadistische organisaties voorbereidingen treffen om in Europa aanslagen te plegen (NCTV, 2023c).
- De enkele honderden Nederlanders die rechts-terroristisch gedachtegoed verspreiden worden steeds

⁴ Tussen het thema 'zorgwekkend gedrag en radicalisering' en 'sociale veiligheid' zit een relatief grote mate van overlap. In dit Risico- en Dreigingsbeeld is gekozen om risico's en dreigingen onder dit thema te vatten als er sprake is van (1) (bereidheid tot) het gebruik van geweld en/of (2) acties welke ingaan tegen de principes van de democratische rechtsorde.

meer online actief. Het *accelerationisme* – een gewelddadige stroming binnen het rechts-extremisme – is in opkomst en bestaat veelal uit een jonge populatie (NCTV, 2022b).

- De term voor ‘anti-overheidsextremisme’ is veranderd naar ‘anti-institutioneel extremisme’, wat kan betekenen dat er ook meer dreiging uitgaat naar het hoger onderwijs als instituut. Ondanks dat de groep activistische demonstranten is afgenomen zijn er zo’n 100.000 ad-hoc aanhangers (AIVD, 2023a).
- Er gaat geen aantoonbare geweldsdreiging uit van het linksextremisme of dierenrechtenextremisme (NCTV, 2023c). De linkse actiegroep is echter wel gegroeid, wat op de middellange termijn kan zorgen voor een toename in polariserende effecten, intimidatie en illegale acties.

Actuele risico’s en dreigingen

- Diffuse en veelzijdige terroristische dreigingen zijn onvoorspelbaarder doordat steeds meer radicalisering online en individueel plaatsvindt.
- Omdat aanhangers van rechtsextremisme steeds jonger zijn neemt de kans toe dat onderwijsinstellingen hier meer mee te maken krijgen.
- Geweldsincidenten ten gevolge van toenemende polarisering.

Risico’s en dreigingen die waarschijnlijk zullen toenemen

- Geweldsincidenten ten gevolge van geestelijke problematiek door het tekort aan geestelijke gezondheidszorg.
- Illegale acties om bestuurders van HO-instellingen te dwingen stelling te nemen.

➤ **Impact:** gebrek sociale en fysieke veiligheid; aantasting kwaliteit onderwijs en onderzoek.

Risico’s en dreigingen zorgwekkend gedrag en radicalisering in de praktijk

- In september 2023 schiet een student met geestelijke problemen drie mensen dood, waaronder een docent aan de Erasmus-universiteit Rotterdam.
- De Gaza-oorlog leidt vanaf eind 2023 tot hevige discussies en spanningen op universiteiten. Studenten en medewerkers eisen van universiteiten dat zij partij kiezen; Joodse studenten voelen zich onveilig; bij protesten in Groningen worden ramen van de universiteitsbibliotheek beschadigd (NOS, 2024a).

Gebouwveiligheid, beveiliging en BHV

Gebouwveiligheid, beveiliging en BHV. Gebouwveiligheid is de mate waarin medewerkers, studenten en derden zich veilig kunnen voelen in een gebouw. Daarbij zijn onder meer de fysieke beveiliging, brandveiligheid, laboratoriumveiligheid en bedrijfshulpverlening (BHV) betrokken (IVHO & COT, 2021).

Ontwikkelingen sinds 2021

- Door toenemende klimaatverandering ontstaan vaker extreme weersomstandigheden, zoals extreme regenval, overstromingen, en droogte. De waarschijnlijkheid van verstoring van vitale infrastructuur door een natuurlijke oorzaak zal dan ook steeds verder toenemen (ANV, 2022).
- De energietransitie, in combinatie met geopolitieke ontwikkelingen, leidt tot grotere inzet op elektrificatie en veranderingen in de manier waarop elektriciteit wordt geproduceerd en gedistribueerd. Met name in de transitiefase kan dit leiden tot onverwachte effecten op en ontwrichting van het elektriciteitsnet (ANV, 2022).
- Technologische ontwikkelingen, innovaties en een steeds meer data-gedreven samenleving bieden kansen voor het ontwikkelen van smart buildings en betere informatie- en veiligheidsvoorzieningen. Echter maakt het instellingen ook afhankelijker van technologieën en daardoor kwetsbaarder, bij-

voorbeeld door het uitvallen van technologieën of digitale systemen wat onder andere risico's voor de fysieke veiligheid met zich meebrengt.

- Er is sprake van toenemend activisme op hoger onderwijsinstellingen. Dit kan leiden tot intimiderende bijeenkomsten op HO-instellingen, waarbij derden kunnen proberen de instellingen binnen te komen, of zelfs bezettingen van hoger onderwijsgebouwen.
- Door de toename in het aantal medewerkers dat thuis werkt kan er mogelijk een tekort aan BHV'ers zijn op locatie (Rondetafelgesprekken).
- De groeiende kamernood in diverse grote studentensteden leidt tot een grotere acceptatie van onveilige woonsituaties. HO-instellingen zijn weliswaar niet verantwoordelijk voor de huisvesting van studenten, maar risico's en ongelukken op dit vlak hebben desalniettemin een potentiële impact op de instelling.

Actuele risico's en dreigingen

- Verstoring kritieke infrastructuur door incidenten en moedwillige acties binnen en buiten de hoger onderwijsinstelling.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Verstoring kritieke infrastructuur door milieu- en energietransitie en door kwaadwillende actoren. Risico's zullen meer dynamisch worden in plaats, soort, omvang en tijd (NIPV, 2022).

➤ **Impact:** Aantasting gebouw- en fysieke veiligheid.

Risico's Gebouwveiligheid, BHV en fysieke veiligheid in de praktijk

- Brandweer Midden-Holland maakt zich ernstig zorgen over brandveiligheid van 20 tot 25 procent van de studentenhuizen in de regio (Omroep West, 2023).
- Een hevige stroomstoring in een gebouw van de Hogeschool Utrecht (HU) op het Science Park leidde tot het besluit de locatie voor een week te sluiten en onderwijs en tentamens elders en/of online te verzorgen (Voets, 2022).
- De politie heeft maandagavond een einde gemaakt aan de bezetting van een deel van het Binnengasthuis van de UvA. Eerder op de dag werd het bezet, omdat de actievoerders willen dat de universiteit haar banden met Shell verbreekt (Van Dongen & Dominicus, 2023).

Internationalisering

Internationalisering betreft de integratie van een internationale, interculturele of mondiale dimensie in de doelen, functies en overdracht van het (hoger) onderwijs op het niveau van de student, de medewerker, het instituut en/of op nationaal niveau (Knight, 2008; Slappendel-Henschen, 2022).

Ontwikkelingen sinds 2021

- Er heeft een enorme instroom van internationale studenten plaatsgevonden, met name in het wetenschappelijk onderwijs. Dit komt mede door het grote Engelstalige onderwijsaanbod. De herinvoering van de basisbeurs per studiejaar 2023/2024 maakt het mogelijk aantrekkelijker voor buitenlandse studenten uit EU/EER-landen om in Nederland te studeren (Dijkgraaf, 2023a; Demirel et. al., 2024).
- Dit leidt bij sommige studies tot overvolle collegezalen en hoge werkdruk bij docenten, waardoor de onderwijskwaliteit onder druk komt te staan. Daarnaast dreigt de toegankelijkheid voor Nederlandse studenten bij verschillende Engelstalige opleidingen in het gedrang te komen. In de grote steden draagt de instroom bij aan gebrek aan studentenhuisvesting (Dijkgraaf, 2023a).
- Niet alle HO-instellingen zijn het eens met en/of ervaren de negatieve effecten van internationalisering: bij HBO-instellingen is de instroom van buitenlandse studenten juist veelal in balans en ook voor

sommige WO-instellingen zou een rem op instroom van internationale studenten problematisch zijn (Smaling, 2023).

- In reactie op deze recente ontwikkelingen heeft de Vereniging Hogescholen een voorstel voor zelfregie op de instroom van internationale studenten aangeboden aan de Minister van OCW (VH, 2024). Ook de universiteiten werken aan beleid om meer evenwicht te brengen in internationalisering en de instroom van internationale studenten. Zo wordt onder andere het aantal Engelstalige opleidingen met een derde teruggebracht (UNL, 2024c).
- Het Ministerie van OCW werkt aan een voorstel 'Wet Internationalisering in Balans' die de Minister van OCW mogelijkheden biedt om in te grijpen wanneer de zelfregie van instellingen niet tot het gewenste resultaat leidt.

Actuele risico's en dreigingen

- Sociale problematiek en discriminatie, met name bij studenten buiten Europa.
- Deelname aan activiteiten die een inbreuk maken op kennisveiligheid (*insider threat*).
- Bij toename internationale studenten bij universiteiten die een te grote instroom ervaren:
 - Afname onderwijskwaliteit
 - Afname toegankelijkheid voor Nederlandse studenten
 - Tekort aan huisvesting in grote steden

- Bedreiging fysieke veiligheid bij uitgaande mobiliteit naar gebieden met spanningen.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Incidenten rondom internationale studenten in Nederland en Nederlandse studenten in het buitenland door toenemende geopolitieke spanningen.

- **Impact:** sociale veiligheid, fysieke veiligheid, kwaliteit onderwijs en onderzoek.

Risico's en dreigingen internationalisering in de praktijk

- Een studie concludeert dat internationale studenten van etnische minderheden die niet uit Europa komen bij medische opleidingen aan Universiteit Maastricht racistisch gedrag ervaren van zowel artsen als patiënten (Science Guide, 2023).
- Achttien EUR-studenten die op uitwisseling waren in Israël, zijn teruggekeerd naar Nederland. Twee andere EUR-studenten zijn nog in Israël, maar zijn veilig (Smaling, 2023).

Cyberveiligheid

Cyberveiligheid betreft de mate waarin (online) informatie beschikbaar, integer en vertrouwelijk is. De beveiligingsmaatregelen voorkomen ongewenste zaken als cybercrime, wijziging van data of onbevoegde openbaarmaking van digitale informatie. Het normenkader SURF audit, gebaseerd op ISO27002:2013, is het kader dat in de sector wordt gebruikt (IVHO & COT, 2021; Rondetafelgesprekken).

Ontwikkelingen sinds 2021

- Het in 2023 door SURF gepubliceerde *Cyberdreigingsbeeld 2023* rapporteert:
 - Het aantal cyberincidenten blijft stijgen; de meeste incidenten vonden plaats bij verkrijging en openbaarmaking van informatie.
 - De belangrijkste incidenten betreffen *ransomware*, *zero-day* kwetsbaarheden en verstoring van cloud-diensten. Aanvallen met gijzelsoftware worden steeds vaker ingezet met dubbele of zelfs driedubbele afpersing.
 - Er worden steeds meer kwetsbaarheden gevonden in systemen en applicaties
 - Weerbaarheid blijft een aandachtspunt, met name waar het gaat om richtlijnen voor menselijk handelen en processen voor samenwerkingsverbanden en ketenpartners.

- Er zijn nog maar weinig instellingen die risico-gebaseerd werken en risico-eigenaarschap is nog beperkt ingebed bij het hogere management.
- Instellingen werken momenteel, met extra middelen die het Ministerie van OCW beschikbaar heeft gesteld, aan de ontwikkeling en implementatie van beleidsmaatregelen die de informatiebeveiliging versterken.
- Toename van digitale spionage door statelijke actoren met als doel verkrijging van hoogwaardige technologie (AIVD, NCTV & MIVD, 2022).

Actuele risico's en dreigingen

- Spionage en openbaarmaking van informatie door statelijke actoren, cybercriminelen, hacktivisten en mensen binnen organisaties die onbedoeld incidenten veroorzaken.
- Sabotage en verstoring diensten, bijvoorbeeld cloud-diensten.
- Bewust beschadigen van imago van de kennisinstelling als onderdeel van een cyberaanval met *ransomware*.
- Onvoldoende aandacht voor cyberrisico's bij onderwijs en bedrijfsvoering.
- Te weinig tijd voor operationele taken door de grote hoeveelheid audits en papierwerk.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Tekortschieten cyberweerbaarheid door gebrek aan expertise om informatie-beveiligings- en privacytaken uit te voeren.
- Het genereren van malware door generatieve AI.
- Cyberspionage door statelijke actoren.
- Schade van incidenten elders in het ecosysteem waar de HO-Instelling deel van uitmaakt.

➤ **Impact:** bedrijfsvoering, kennispositie, sociale en fysieke veiligheid, integriteit

TekortRisico's en dreigingen cyberveiligheid in de praktijk

- In 2022 werden na een hack bij een leverancier van toegangspassen de persoonsgegevens van duizenden medewerkers en studenten van meerdere kennisinstellingen op het Dark Web gepubliceerd (Teunis, 2022; SURF 2023a).
- Studenten hebben in 2023 een kwetsbaarheid ontdekt in de beveiliging van de TU Delft mail. Hierdoor was het mogelijk om e-mails te versturen uit naam van een ander verbonden aan de universiteit (Van der Veldt, 2023).

- Na een cyberaanval op IT-bedrijf NEBU zijn mogelijk klantgegevens van 2,5 miljoen mensen gelekt (RTL Nieuws, 2024). Hierbij zijn ook onderwijsinstellingen betrokken (Weerwind & Van Huffelen, 2023).

Privacy

Privacy van informatie gaat over het registreren en verwerken van (persoons)gegevens en over het verbod voor derden om zonder toestemming informatie over een persoon te verkrijgen. Het betreft ook het voorkomen dat er onnodig informatie bij anderen terecht komt en wordt opgeslagen. De Algemene Verordening Gegevensbescherming (AVG) is een belangrijke norm (IVHO & COT, 2021). Daarnaast gebruikt de sector het SURFaudit toetsingskader privacy (Rondetafelgesprekken).

Ontwikkelingen sinds 2021

- De onderwijssector heeft zich sterk ingezet om 'privacy compliance' te verhogen. Bewustzijn met betrekking tot privacy in onderwijs en onderzoek is sinds 2021 ook licht verbeterd (AP, 2024).
- Versnelde digitalisering en toename hybride werken versterken risico's met betrekking tot privacygevoelige informatie.

- Er is een *Collaborative Trust Framework* ontwikkeld dat principes en verantwoordelijkheden beschrijft van digitale technologie voor het onderwijs, hieronder valt ook intelligente technologie. In het raamwerk is er specifiek aandacht voor de impact op privacy (Onderwijsraad, 2022).
- Onderwijsinstellingen krijgen meer te maken met maatschappelijke kwesties, zoals bijvoorbeeld zorgtaken rondom mentale gezondheid. Voor de verwerking van deze persoonsgegevens is mogelijk geen AVG-grondslag (AP, 2024; Rondetafelgesprekken).
- Nieuwe ontwikkelingen in algoritmes & artificiële intelligentie vragen om beleid; zo zijn er bijvoorbeeld zorgen over verzamelen en verwijderen van persoonsgegevens bij het gebruik van taalmodellen zoals ChatGPT (SURF, 2023b).
- Een toename in het gebruik van adaptieve leermiddelen en *'learning analytics'* door onderwijsinstellingen leidt tot een toename van gegevens over het gedrag en de ontwikkeling van leerlingen en studenten. Deze data kunnen verkeerd geïnterpreteerd worden en of onveilig beheerd worden (AP, 2024).
- HO-instellingen kunnen data gebruiken om met behulp van *'student analytics'* hun onderwijs te verbeteren, bijvoorbeeld met een programma zoals het Amerikaanse Canva. Bij deze toepassing zijn er zorgen over de hoeveelheid data dat private bedrijven daarmee verzamelen en verwerken (Rathenau Instituut, 2022).
- De aankomende AI-Verordening zal van HO-instellingen aanpassingen vergen op het gebied van nor-

men bij het ontwikkelen, implementeren of updaten van systemen of toepassingen (AP, 2024).

Actuele risico's en dreigingen

- Onvoldoende overzicht over alle verwerkingen van persoonsgegevens binnen kennisinstellingen door de autonome positie van docenten, de 'wildgroei' aan software en de soms grote hoeveelheid onderzoeken en samenwerkingen met andere organisaties (AP, 2024).
- Onvoldoende herkenning en melding van datalekken.
- Schending AVG bij het verwerken van persoonsgegevens voor onderzoek.
- Het is een uitdaging voor kleinere instellingen om te voldoen aan de AVG wegens beperkingen in geld en capaciteit.
- Gebrek aan dataminimalisatie (bewaar- en vernietigingsbeleid) waardoor er nog meer data lekt.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Misbruik en/of schending van AVG van gegevens die worden gegenereerd bij het toenemend gebruik van adaptieve leermiddelen en *'learning analytics'*.
- Misbruik sensitieve informatie die is opgeslagen door clouddiensten (Okano-Heijmans, 2023).

➤ **Impact:** integriteit, sociale veiligheid, kwaliteit onderwijs en onderzoek.

Risico's en dreigingen rondom privacy in de praktijk

- Na protesten zet Universiteit Leiden de omstreken *'class room scanners'*, die het aantal aanwezigen telden, uit om zorgen over privacy (AD, 2021).

Kennisveiligheid en ongewenste beïnvloeding

Kennisveiligheid en ongewenste beïnvloeding betreft het voorkomen van ongewenste overdracht van sensitieve kennis en technologie met negatieve gevolgen voor onze nationale veiligheid en de Nederlandse innovatiekracht. Daarnaast gaat het om het tegengaan van heimelijke beïnvloedings- en inmengingsactiviteiten van statelijke actoren in hoger onderwijs en wetenschap. Dergelijke beïnvloeding (*foreign interference*) kan leiden tot vormen van (zelf)censuur resulterend in aantasting van de academische vrijheid. Tot slot draait het om ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd (UNL, 2022).

Ontwikkelingen sinds 2021

- De overheid waarschuwt steeds explicieter dat Nederlandse kennisinstellingen aantrekkelijke doelwitten zijn voor landen die op zoek zijn naar hoogwaardige technologieën en kennis. De AIVD noemt China de grootste dreiging voor kennisveiligheid, maar wijst ook naar Rusland en Iran (AIVD, 2023a; AIVD, 2024).
- De diensten treden steeds vaker handelend op om cyberaanvallen op onder andere technische universiteiten te voorkomen (Twigt, 2024).
- De afgelopen jaren is er veel beleid rondom kennisveiligheid ontwikkeld door OCW alsook Rijksbreed:
 - Nationale Leidraad Kennisveiligheid (2022; herziening in 2024), die handvatten geeft om kansen en risico's bij internationale samenwerking af te wegen.
 - Oprichting van het Loket Kennisveiligheid waar kennisinstellingen terecht kunnen en advies kunnen vragen over internationale samenwerkingsprojecten.
 - Er wordt gewerkt aan een wetsvoorstel 'screening kennisveiligheid' om onderzoekers en studenten buiten de EER die in een risicovakgebied willen werken/studeren te screenen.
- De ontwikkeling van kennisveiligheidsbeleid bij universiteiten is voornamelijk gericht op het voorkomen van de ongewenste overdracht van sensitieve kennis en technologie en minder op heimelijke beïnvloeding en ethische kwesties (AP, 2024).

Actuele risico's en dreigingen

- Spionage, ongewenste kennisoverdracht en inbreuk op IP-rechten op strategische kennisgebieden waarin kennisinstellingen vooroplopen. Dergelijke risico's en dreigingen nemen toe wanneer deze onderschat worden en de kennisveiligheidsmaatregelen onvoldoende effectief zijn.
- Inbreuk op academische vrijheid, ongewenste beïnvloeding, en stimuleren van zelfcensuur door niet-democratische landen.
- Inbreuk op ethische normen met betrekking tot wetenschappelijk onderzoek, bijvoorbeeld in de vorm van 'ethics dumping'.
- Risico op overregulering en daardoor een hoge werkdruk.

Risico's en dreigingen die waarschijnlijk zullen toenemen

- Spionage en kennisdiefstal, onder meer met behulp van generatieve AI.
- Waterbedeffecten:
 - Door de oorlog met Oekraïne zal Rusland nog meer interesse hebben om op heimelijke manieren (kennis over) technologieën te vergaren.
 - Wanneer er veel wordt gedaan aan kennisveiligheid nemen de risico's van ongewenste beïnvloeding en inbreuk op

sociale veiligheid toe. Zo houdt screening onderzoekers met kwade bedoelingen buiten de deur, wat kan leiden tot meer beïnvloeding omdat statelijke actoren dan meer inzetten op wie er al binnen is bij een instelling. Ook kan dit leiden tot meer cyber-activiteiten.

➤ **Impact:** kennispositie van instellingen, kwaliteit van onderwijs en onderzoek.

Risico's en dreigingen kennisveiligheid en ongewenste beïnvloeding in de praktijk

- De Vrije Universiteit Amsterdam sluit een door China gefinancierd Mensenrechten-centrum nadat een onafhankelijke commissie concludeert dat de onderzoekers zich kwetsbaar hebben gemaakt voor politieke beïnvloeding. Verder plaatsen zij vraagtekens bij de inhoud en methodologie van hun onderzoek (Commissie Stolker, 2022).
- De AIVD wist in 2022 in enkele gevallen te voorkomen dat onder meer Rusland en Iran materialen, techniek en (toegepaste) wetenschappelijke kennis uit Nederland bemachtigden die ze hadden kunnen gebruiken voor hun nucleaire programma's (AIVD, 2023a).



NIET ENKEL WORDT HET
LANDSCHAP **BREDER EN DIFFUSER**,
OOK RAKEN OGENSCHIJNLIJK
APARTE **RISICOCATEGORIEËN**
STEEDS MEER MET ELKAAR
VERWEVEN.



HET RISICO-
EN DREIGINGS-
LANDSCHAP:
VIJF
BELANGRIJKE
(TOEKOMSTIGE)
TRENDS

3 HET RISICO- EN DREIGINGSLANDSCHAP: VIJF BELANGRIJKE (TOEKOMSTIGE) TRENDS

Het risico- en dreigingslandschap voor hoger onderwijsinstellingen wordt steeds complexer en uitdagender door veranderende sociale dynamieken, de snelle vooruitgang van technologieën en toenemende geopolitieke spanningen. Niet enkel wordt het landschap breder en diffuser, ook raken ogenschijnlijk aparte risicocategorieën steeds meer met elkaar verweven. HO-instellingen kunnen zich niet langer enkel beperken tot het overbrengen en genereren van kennis, ze krijgen namelijk in steeds grotere mate te maken met maatschappelijke en (geo)politieke kwesties waarop zij geacht worden te acteren en reageren. Bovendien komt er steeds meer regelgeving rondom risico's, wat grote veranderingen teweeg kan brengen in hoe integrale veiligheid wordt nagestreefd.

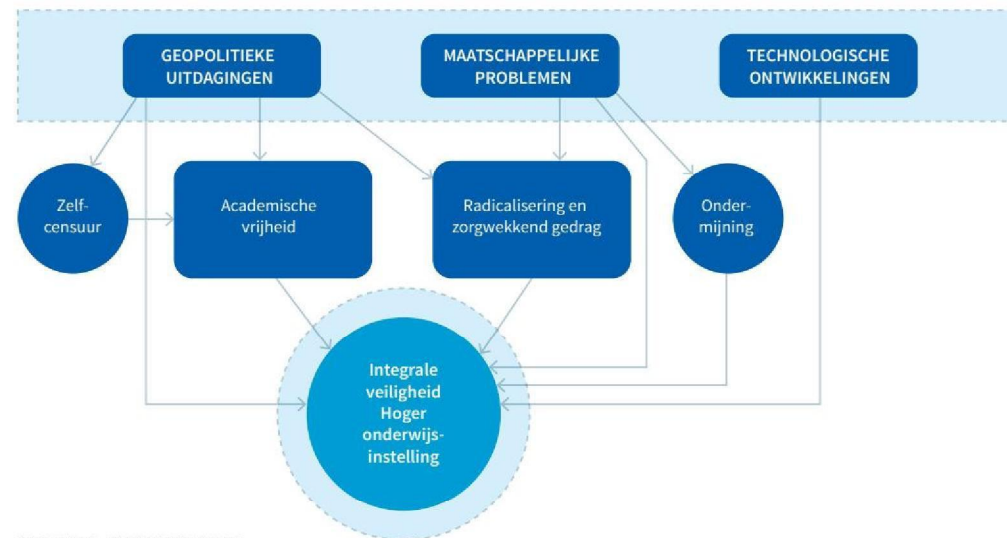
Uit het onderzoek komen verschillende bredere ontwikkelingen naar voren die een impact hebben op risico's en dreigingen voor het hoger onderwijs. Hieronder worden vijf meest impactvolle trends geschetst, waarop sinds het uitkomen van het laatste Risico- en Dreigingsbeeld veel beweging is geweest en waarop ook in de komende jaren veel (nieuwe) ontwikkelingen worden verwacht.

De twee belangrijkste overkoepelende ontwikkelingen zijn de veranderende internationale omgeving – geopolitieke competitie, internationale conflicten en crises – en de groeiende maatschappelijke uitdagingen die zich vertalen in risico's, dreigingen en dilemma's

voor het hoger onderwijs. De grootste fysieke veiligheidsdreiging gaat uit van radicalisering en zorgwekkend gedrag, een thema dat nauw verweven is met geopolitieke ontwikkelingen en politisering van de wetenschap. De impact van opkomende technologieën is voornamelijk nog onduidelijk, maar is potentieel zeer groot en raakt aan veel veiligheidsthema's in alle domeinen. Beknotting van academische vrijheid is de minst tastbare van de vijf trends en heeft juist daarom meer aandacht: de impact ervan op de lange termijn op de kwaliteit van onderwijs en onderzoek kan groot zijn en daarmee de positie en het concurrentiepositie van HO-instellingen aantasten.

GEOPOLITIEKE COMPETITIE, INTERNATIONALE CONFLICTEN EN CRISES HEBBEN STEEDS MEER IMPACT OP HET HOGER ONDERWIJS

We leven in een geopolitiek turbulente tijd. De wereld beweegt toe naar een multipolair systeem dat gekenmerkt wordt door toenemende competitie, (gewapend) conflict en crises alsook verschuivende machtsverhoudingen. Toenemende geopolitieke en geo-economische competitie, internationale conflicten en crises hebben steeds meer invloed op onze binnenlandse economie en de maatschappij. Handelsbeleid is in toenemende mate gepolitiseerd en protectionis-



FIGUUR 2. VERWEVENHEID
IMPACTVOLLE ONTWIKKELINGEN OP HOOFDLIJNEN.

tische maatregelen nemen toe. Zo raken geopolitieke en geo-economische ontwikkelingen steeds verder met elkaar verstrengeld.

Ook het hoger onderwijs, dat in de afgelopen jaren sterk geïnternationaliseerd is, wordt in toenemende mate door geopolitieke ontwikkelingen en internationale conflicten geraakt. Enerzijds omdat kennis een strategisch machtsmiddel is geworden en de rol van het hoger onderwijs als succesfactor in de ontwikkeling van een kenniseconomie wordt gezien. Anderzijds omdat er dankzij de internationalisering van het hoger onderwijs veel internationale studenten in Nederland onderwijs volgen en/of onderzoek doen, inclusief uit landen waar de conflicten zich afspelen.

Er zijn legio recente voorbeelden van hoe dit directe invloed heeft op het hoger onderwijs. Zo heeft de Russische invasie van Oekraïne in 2022 een mondiale geopolitieke schok veroorzaakt waardoor westerse landen en Rusland lijnrecht tegenover elkaar zijn komen te staan. In het hoger onderwijs werd alle samenwerking met Rusland van het ene op het andere moment stopgezet. Een ander voorbeeld betreft de grootmacht competitie tussen de Verenigde Staten en China, met name waar het gaat om de strijd om wetenschap en technologie. Europa en Nederland worstelen met de vraag hoe deze competitie zich verhoudt tot hun eigen zorgen over economische en kennisveiligheid in de samenwerking met China. Ook de oorlog in Gaza en

de toenemende onrust in het Midden-Oosten hebben rechtstreeks impact op het hoger onderwijs in Nederland. Deze impact is zowel te zien op het academische debat, wat sterk gepolariseerd is door de oorlog, als op sociale veiligheid en de omgang met activisme op de campus (Bekkers, Aartsma & Sweijs, 2024; AIVD, MIVD & NCTV, 2022).

Als gevolg van deze ontwikkelingen zien landen en kennisinstellingen de laatste jaren toenemende risico's op het gebied van strategische afhankelijkheden, kennisdiefstal, en beïnvloeding en ondermijning door statelijke actoren, ook waar het gaat om academische vrijheid. Bovendien lijken spionage- en beïnvloedingsactiviteiten door statelijke actoren in de nabije toekomst eerder toe- dan af te nemen (Aartsma & Dijkman, 2024; ANV, 2022). Deze trend van politisering van de wetenschap en bredere geopolitieke invloeden op het hoger onderwijs zal zich daarom naar verwachting de komende jaren voortzetten of zelfs uitbreiden.

MAATSCHAPPELIJKE PROBLEMEN LEIDEN TOT STEEDS MEER DRUK OP HO-INSTELLINGEN, WAT DE ROL EN POSITIE VAN HET HOGER ONDERWIJS AANTAST

Een groeiend aantal maatschappelijke ontwikkelingen werken door in het hoger onderwijs. In steeds meer gevallen komen problemen ongewild en onbedoeld op het bord van onderwijsinstellingen te liggen. Dat geldt voor ondermijning – de negatieve effecten van georganiseer-

de criminaliteit – maar ook voor het groeiend beroep dat op HO-instellingen wordt gedaan om te reageren en/of acteren op (geo-)politieke conflicten en maatschappelijke problematiek zoals de hoge druk op psychische en mentale zorg voor studenten en stafleden.

Eén van de maatschappelijke problemen is de vermenging van onder- en bovenwereld ofwel de in-nesteling van de georganiseerde criminaliteit in de maatschappij. Het gaat criminele organisaties om het verdienen van geld maar hun activiteiten hebben vaak ondermijnende effecten op de maatschappij, inclusief in het hoger onderwijs. Deze ondermijning ten gevolge van criminele activiteiten is een relatief nieuw thema binnen integrale veiligheid van hoger onderwijsinstellingen. Het betreft namelijk een sluimerend proces en de cases zijn vaak gevoelig, waardoor de problematiek gemakkelijk onder de radar kan blijven. Niettemin onderkennen steeds meer HO-instellingen deze problematiek (Rondetafelgesprekken). Gevallen van ondermijning in het hoger onderwijs betreffen afpersing, witteboordencriminaliteit zoals het faciliteren van of meewerken aan het witwassen van geld, belastingontduiking, of diploma fraude, en/of spelen zich af op het terrein van drugshandel. Zowel medewerkers als studenten kunnen hierbij betrokken raken.

Waar het gaat om afpersing zijn vooral internationale studenten die (nog) niet goed de weg weten in Nederland kwetsbaar (Rondetafelgesprekken). Met

betrekking tot de drugshandel gaat het om activiteiten zoals bijvoorbeeld het ronselen van scheikunde-studenten om te werken in synthetische drugslabs of het financieel ondersteunen van studenten om hen later te dwingen een criminele organisatie te helpen bij bedrijfsvoering. Ook komt het voor dat criminelen zich inschrijven voor studies om zo gemakkelijker in contact te komen met studenten. Deze praktijk kan zich gemakkelijk doorzetten in de toekomst: zo er is een toename van dealers onder studenten gesignaleerd (van der Torre et. al., 2023, p. 36-37). Deze ontwikkeling heeft mogelijk impulsen gekregen door de algehele toename van drugsgebruik onder studenten, de verschuiving van horeca naar scholen in de coronatijd, en de afname in het 'invliegen' van Zuid- en Midden-Amerikaanse koks van drugs (Frankenhuis, 2023). Op het gebied van witteboordencriminaliteit komen niet alleen wetenschappelijke stafleden in aanraking met schimmige activiteiten – denk aan de samenwerking van sommige fiscale wetenschappers met belastingadvieskantoren aan de Zuidas om behulpzaam te zijn bij belastingontwijking (Baazil, 2024) – maar ook studenten die stagelopen en ogenschijnlijk onschuldige hulp bieden aan louche bedrijven of organisaties, veelal op juridisch-economisch gebied. Tot slot vindt er ook inmenging en ondermijning 'by proxy' plaats, bijvoorbeeld wanneer een staat een criminele organisatie gebruikt om ondermijningsdoelen te behalen, of een criminele organisatie een commercieel bedrijf. Ondermijning heeft de potentie om sluipenderwijs

de fundamenteën van de rechtsstaat aan te tasten en daarmee ook de veiligheid en integriteit van de samenleving. In het verlengde daarvan ondergraven deze ontwikkelingen de veiligheid, integriteit en het imago van de kennisinstelling, alsmede de effectiviteit van onderwijs. Kennisinstellingen voelen dan ook steeds meer de druk om hierop te acteren (Rondetafelgesprekken).

Niet alleen ontwikkelingen op het gebied van criminele ondermijning behoeven aandacht van HO-instellingen. Ook geopolitieke en andere maatschappelijke ontwikkelingen en problemen vragen steeds meer aandacht van besturen en medewerkers en leiden daarmee af van hun primaire taken. Zo is er ten eerste steeds meer druk op besturen om stelling te nemen ten aanzien van conflicten (denk aan de Gaza-oorlog) en maatschappelijke kwesties (denk aan klimaat of gendervraagstukken). Dit terwijl zij het juist als hun taak zien om het open academisch debat daarover te stimuleren. Ten tweede vinden er onregelende acties van statelijke en niet-statelijke actoren plaats, zoals bijvoorbeeld inbreuk op kennisveiligheid door Rusland en China (denk aan algemene hackactiviteiten en hackactiviteiten gericht op het frustreren van specifiek onderzoek).

Daarnaast moet er ook gehandeld worden ten aanzien van kwesties als snelle technologische ontwikkelingen, het gebrek aan mankracht en expertise op het terrein van veiligheidskwesties en ICT, en de toenemende psy-

chische problematiek rondom medewerkers en studenten (Ten Have et. al., 2022). Dit laatste treft vooral ook buitenlandse studenten, die vaak minder gemakkelijk toegang hebben tot geestelijke gezondheidszorg (Rondetafelgesprekken). Hier geven HO-instellingen aan dat de druk om als vangnet te fungeren voor het overbelaste nationaal geestelijk zorgsysteem snel groeit, bijvoorbeeld waar het gaat om studenten die wegens de lange wachttijden voor geestelijke gezondheidszorg nergens anders met hun psychische problematiek terecht kunnen. Steeds vaker ondernemen medewerkers actie omdat zij een zorgplicht voelen wanneer andere instanties tekortschieten. Sinds het vorige Risico- en Dreigingsbeeld in 2021 zijn de wachttijden van diverse diagnosegroepen nog verder opgelopen, van ongeveer 21 weken naar 27 weken in 2023 (Landelijke stuurgroep toegankelijkheid en wachttijden ggz, 2023). Naar verwachting zullen de wachttijden, zeker voor de meest complexe problematiek, niet snel afnemen in de komende jaren.

HO-instellingen moeten dus, vaak noodgedwongen, steeds meer additionele taken op zich nemen waarvoor zij in mindere mate of niet zijn ingericht en waarvoor zij weinig tot geen capaciteit hebben. In combinatie met de groeiende druk op besturen om te reageren op internationale en nationale kwesties neemt dit de aandacht weg van primaire onderwijs- en onderzoekstaken, en komen er steeds meer taken bij met betrekking tot integrale veiligheid en risicoma-

nagement. Tezamen vormt dit een risico voor de kwaliteit van onderwijs, onderzoek, en veiligheid.

TOENEMENDE RADICALISERING EN ZORGWEKKEND GEDRAG VORMEN EEN DREIGING VOOR DE VEILIGHEID VAN HO-INSTELLINGEN

Toenemende radicalisering en zorgwekkend gedrag vormen een groeiende dreiging voor de veiligheid van hoger onderwijsinstellingen. Deze dreiging wordt onderstreept door verschillende ontwikkelingen die in recente rapporten van veiligheidsinstanties zijn belicht. Zo wordt al geruime tijd een stijging waargenomen in terroristische dreiging. Eind 2023 bevestigde de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) deze trend door het dreigingsniveau te verhogen van niveau 3 (voorstelbaar) naar niveau 4 (reëel). Dit niveau was sinds 2019 onveranderd gebleven. Niet alleen is de algemene dreiging toegenomen, ook het percentage jonge terrorismeverdachten neemt gestaag toe (NCTV, 2023c). Zodoende is het niet ondenkbaar dat gewelddadige acties zich af kunnen spelen op hoger onderwijsinstellingen – ook omdat deze instellingen, ondanks extra veiligheidsmaatregelen die al op verschillende plekken zijn ingevoerd, *soft targets*⁵ zijn. Het feit dat het percentage jonge terrorismeverdach-

⁵ Soft targets zijn locaties die relatief gemakkelijk toegankelijk zijn voor het grote publiek en relatief onbeschermd zijn, waardoor ze een gemakkelijk doelwit zijn voor o.a. terroristische aanslagen.



ten toeneemt is deels te verklaren vanuit het feit dat zowel jihadistische als rechtsextremistische groepen steeds meer gebruik maken van online kanalen voor de verspreiding van propaganda en het aantrekken van nieuwe sympathisanten. Hierbinnen vormen jihadistisch gemotiveerde individuen en groepen al jaren een ernstige geweldsdreiging (AIVD, 2024). Zij maken gebruik van internationale conflicten (zoals de Gaza-oorlog) en koranschendingen om sympathisanten aan te moedigen tot aanslagen in westerse landen. Recente arrestaties in Nederland en aanslagen in naburige landen onderstrepen de reële risico's die hieraan verbonden zijn. Tegelijkertijd bestaat ook de mogelijkheid dat (voornamelijk) eenlingen vanuit het rechtsextremistische gedachtegoed overgaan tot geweld of een aanslag (AIVD, 2024). Echter is deze scene in Nederland relatief diffuus en over het algemeen minder geneigd tot gewelddadige acties. Wat echter een alarmerend aspect toevoegt aan dit risico voor hoger onderwijsinstellingen, is dat met name binnen het rechtsextremistisch gedachtegoed interesse wordt geuit voor schietpartijen op scholen (NCTV, 2023c, p. 26).

Vanuit het linksextremisme en dierenrechtenextremisme gaat momenteel geen aantoonbare geweldsdreiging uit (NCTV, 2023c), en vanuit het anti-institutionalisme slechts beperkt (AIVD, 2023b; AIVD, 2024). Desalniettemin is de linkse actie-scene gegroeid, en proberen anarchistische en antifascistische groepen vaker rechtse personen en groepen te intimideren

(AIVD, 2024). Dergelijke acties kunnen, samen met het narratief vanuit het anti-institutionalisme, een sfeer van bedreiging, intimidatie en intolerantie creëren. Dit kan op de langere termijn bijdragen aan de ondermijning van de democratische rechtsorde en het hoger onderwijs, zoals in de vorige trend ook is beschreven. Eveneens is er een groeiende soevereiniteitsbeweging in Nederland, voortkomend uit de bredere anti-institutionele beweging. Alhoewel hun acties meestal geweldloos zijn neemt de mate van intimidatie en bedreiging, onder meer naar wetenschappers, de laatste tijd toe (AIVD, Nationale Politie & NCTV, 2024).

Hoger onderwijsinstellingen zijn traditioneel een broedplaats voor het delen en uitdagen van verschillende wereldbeelden en culturen. Dialoog en diversiteit staan daarbij centraal. Echter vormt de toename in radicalisering en zorgwekkende gedragingen, zeker in combinatie met de druk op de geestelijke gezondheidszorg en de invloed van ondermijning op het hoger onderwijs, een substantiële bedreiging voor de fysieke en sociale veiligheid van studenten en medewerkers.

TECHNOLOGISCHE ONTWIKKELINGEN BRENGEN NIEUWE RISICO'S EN DREIGINGEN MET ZICH MEE EN KUNNEN BESTAANDE RISICO'S EN DREIGINGEN VERGROTEN.

De komende jaren gaat het hoger onderwijs steeds meer te maken krijgen met opkomende en disruptie-

ve technologieën – ook wel sleuteltechnologieën genoemd. Dit bevindt zich onder meer op het gebied van AI, quantum en robotica. Deze veranderingen creëren veel kansen, maar ook risico's en dreigingen omdat deze technologieën voor flinke disruptie kunnen en zullen zorgen – ook binnen het hoger onderwijs (EZK, 2024).⁶ Veel technologie wordt steeds breder beschikbaar. Momenteel springen de snelle ontwikkelingen op het gebied van Generatieve AI het meest in het oog: ChatGPT was binnen twee maanden na lancering de snelst groeiende softwareapplicatie ooit (Hu, 2023).

Over de ontwikkeling en uitwerking van nieuwe technologieën bestaat een hoge mate van onzekerheid en onduidelijkheid. HO-instellingen zullen dan ook over grote wendbaarheid en flexibiliteit moeten beschikken om zich succesvol aan te passen aan veranderende omstandigheden. Dit is een grote uitdaging waarbij het risico bestaat dat aanpassingen binnen het hoger onderwijs niet tijdig gerealiseerd (kunnen) worden.

⁶ Waar het gaat om kansen kunnen ze onderwijs- en onderzoekspraktijken versimpelen en versnellen. Dit kan bijvoorbeeld door slimmere analyses van onderwijsresultaten, of door systematische taken die nu veel tijd kosten over te nemen. Er ontstaan in bijna alle vakgebieden onderzoeksmogelijkheden die voorheen ondenkbaar waren. Zo kunnen de technologieën connectiviteit versterken en nieuwe mogelijkheden bieden in het creëren en delen van data en analysemethodes.

Een aantal ontwikkelingen zijn al (deels) zichtbaar:

- a. Nieuwe technologie heeft een grote invloed op de aard en mate van cyberdreiging. Het Cyberdreigingsbeeld 2023 van SURF geeft een overzicht van de dreigingen en kwetsbaarheden en het belang van gedegen weerbaarheid op dit vlak (SURF, 2023aF). De snelle ontwikkelingen op het gebied van Generatieve AI sinds het uitbrengen van dit beeld, zoals bijvoorbeeld het eenvoudig en binnen een oogwenk creëren van content zoals tekst, video en geluid, onderstrepen de snel toenemende risico's op het gebied van informatiebeveiliging, integriteit en privacy nog eens extra.
- b. Ook geeft het een enorme boost aan cybercapaciteiten waardoor de cyberdreiging gericht tegen het hoger onderwijs fors kan toenemen. Dit leidt tot de grote uitdaging om voldoende tech-talent in te huren en tech-capaciteit op te bouwen en te behouden binnen de HO-instellingen. Techtalenten zijn schaars en bedrijven betalen forse salarissen om hen binnen te halen. Ook is het belangrijk om te voorkomen dat het onderwijsbestel (te) afhankelijk wordt van *bigtech*-bedrijven, bijvoorbeeld Google, die het veelgebruikte Google *Workspace for Education* aanbiedt (SURF, 2023c). Ketenafhankelijkheden zullen de komende jaren snel kunnen veranderen mede doordat nieuwe spelers, waaronder commerciële buitenlandse bedrijven, snel dominant kunnen worden.

- c. Generatieve AI maakt nieuwe onderwijsvormen mogelijk, die met nieuwe technologieën binnen handbereik liggen van en voor bijna iedereen. Zo zal generatieve AI steeds beter in staat zijn om bijvoorbeeld een leerprogramma of een game op te zetten waarbij voldaan wordt aan specifieke leerwensen van een individu. Deze applicaties zullen enerzijds geïncorporeerd kunnen worden in het hoger onderwijs maar leveren anderzijds ook verschillende uitdagingen op. Zo is er het risico van *biases* en discriminatie op basis van gender en etniciteit in data en algoritmes, en zouden studenten door (overmatig of verkeerd) gebruik van AI minder creatief kunnen worden of minder gemakkelijk leren om kritisch te reflecteren. Ook maakt intensief gebruik van AI het onderwijs kwetsbaar voor technische (ver)storingen en hacks. Daarnaast kan er een tweedeling ontstaan tussen instellingen en groepen daarbinnen die nieuwe technologie wel in positieve zin weten te omarmen en anderen die daartoe niet in staat zijn. Tot slot zou deze ontwikkeling in de toekomst mogelijk een bedreiging kunnen vormen voor de positie van de huidige HO-instellingen, omdat het met gebruikmaking van AI gemakkelijker kan worden individuele en adaptieve (online) onderwijsmodules te genereren die flexibel en goedkoper door kleinere organisaties aangeboden zouden kunnen worden (Rondetafelgesprekken).

Omgaan met de invloed van snel-opkomende technologieën is zeker geen zaak van alleen IT-afdelingen binnen het Hoger Onderwijs, zij vinden immers hun doorwerking in de gehele organisatie. Daarbij komt de uitdaging dat de verschillende inzet van AI bij de verschillende faculteiten en afdelingen om maatwerk op decentraal niveau vraagt. Tot slot zal het veel kennis en kunde vragen om de legio (nieuwe) kansen die technologie biedt te omarmen en tegelijkertijd risico's en dreigingen in afdoende mate te mitigeren.

TOENEMENDE BEKNOTTING VAN ACADEMISCHE VRIJHEID ONDERGRAAFT EEN FUNDAMENTELE VOORWAARDE VOOR HOOGWAARDIG ONDERWIJS EN ONDERZOEK

Academische vrijheid is een fundamentele voorwaarde voor hoogwaardig onderwijs en hoogwaardige wetenschapsbeoefening. Wetenschappers, docenten en studenten moeten in vrijheid onderzoek kunnen doen en resultaten kunnen publiceren, onderwijs kunnen geven en volgen, en in openheid ideeën kunnen uitwisselen (KNAW, 2021). In Nederland staat academische vrijheid echter al enige jaren onder druk. Alhoewel Nederland op mondiaal niveau goed scoort op academische vrijheid, liggen de Nederlandse rapportcijfers binnen Europa onder het gemiddelde van de EU-lidstaten. Bovendien is de situatie in Nederland in 2023 verder achteruitgegaan (STOA, 2024). Op de lijst van de *Academic Freedom index 2023* staan slechts drie

EU-lidstaten lager dan Nederland. Negatieve trends en ontwikkelingen zijn er met name op de onderdelen vrijheid van academische uitwisseling en verspreiding, campusintegriteit (de mate waarin campussen vrij zijn van politiek gemotiveerde surveillance of inbreuk op veiligheid), financiële autonomie, en academische autonomie (STOA, 2024).

De dreiging lijkt vanuit steeds meer verschillende kanten te komen. De overheid en de politiek mengt zich via financiering en/of wet- en regelgeving in toenemende mate in de inhoud van onderzoek en onderwijs (STOA, 2024). Ook mengen zij zich in het waarborgen van academische vrijheid, terwijl deze taken primair bij onderwijsinstellingen zou moeten liggen (STOA, 2024). Daarnaast bestempelen politici specifiek onderzoek of activiteiten van individuen als ‘activistisch’ of ‘een linkse hobby’. Ook gebruiken zij andere politieke argumenten om te stellen dat bepaalde onderzoeksgebieden niet-wetenschappelijk zijn (bijv. genderstudies) en daarom ook geen financiering behoeven. Deze invloed vanuit de politiek, die de wetenschap in diskrediet kan brengen, kunnen af- of toenemen met wisselende politieke constellaties.

Binnen kennisinstellingen komen de dreigingen van bestuurders die academische vrijheid beknotten ten behoeve van strategische prioriteiten; kennisveiligheidsmaatregelen nemen die zich lastig verhouden tot academische vrijheid; lezingen en bijeenkomsten

over controversiële thema’s verbieden en/of politiek gemotiveerde personele maatregelen nemen. Ook wetenschappers, docenten en studenten proberen soms discussies, onderzoeken, en onderwijs over specifieke thema’s te verhinderen.

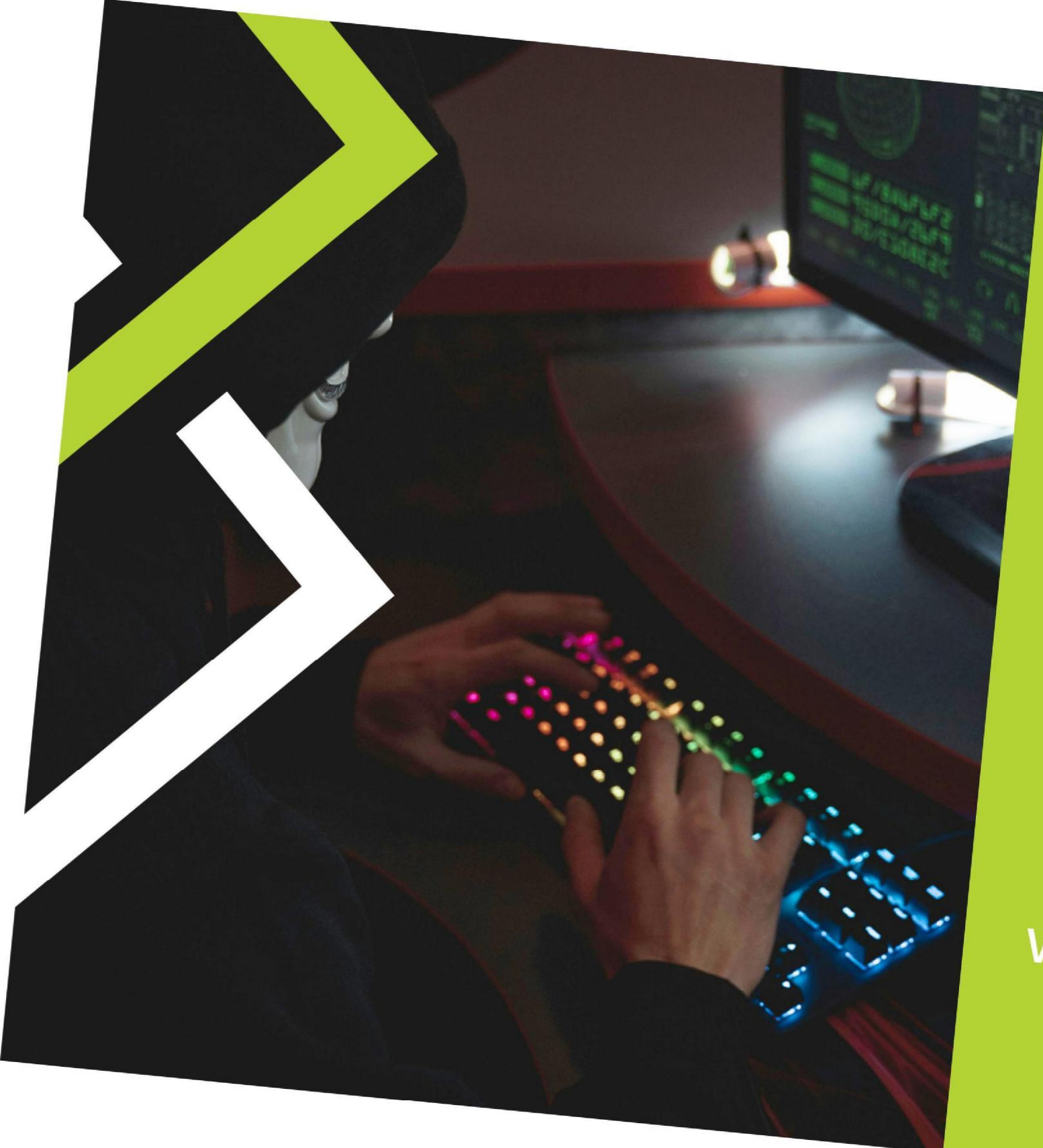
Ook uit maatschappelijke hoek is er sprake van diverse vormen van dreiging. Individuele onderzoekers of onderzoeksgroepen worden, vaak via de sociale media, in toenemende mate bedreigd of verbaal aangevallen vanwege hun onderzoek of bepaalde uitspraken. Ook worden bestuurders in het hoger onderwijs onder druk gezet om kritische geluiden binnen de kennisinstelling te dempen en kritische docenten of studenten het zwijgen op te leggen (STOA, 2024). Financiering van onderzoek en debat door de privésector is vaak thematisch sturend en leidt tot minder ruimte voor vrij en door nieuwsgierigheid gedreven onderzoek.

Op internationaal niveau wordt academische vrijheid beknut door statelijk actoren die via financiering of andere drukmiddelen (bijvoorbeeld verstrekking van visa of toegang tot onderzoeksbronnen) invloed uitoefenen op de inhoud van onderzoek, onderwijs en het debat. Dit werkt zelfcensuur in de hand.

Een deel van de bovengenoemde dreigingen komt mede voort uit toenemende geopolitieke spanningen. Deze ontwikkeling, in combinatie met de groeiende impact van geopolitieke ontwikkelingen op de weten-

schap, zorgt ervoor dat academische vrijheid ook in de komende jaren meer onder druk zal komen te staan. Daarnaast wordt er gesignaleerd dat er in Nederland geen duidelijkheid is over de basisvoorwaarden waaronder academische vrijheid moet worden uitgeoefend (STOA, 2024). Bovenstaande ontwikkelingen kunnen niet los van elkaar worden gezien. De trends rondom geopolitieke en technologische ontwikkelingen, de impact van het tekort aan psychische zorg en ondermijning op HO-instellingen, en de beknotting van academische vrijheid zijn verweven en versterken elkaar vaak.

Daarom vraagt mitigatie van de risico’s om een integrale aanpak. Ook raken zij allen aan de maatschappelijke positie van wetenschap. Die rol is niet langer vanzelfsprekend. Hoewel het vertrouwen in ‘de wetenschap’ groot is, en er naar wetenschappers wordt gekeken voor het oplossen van problemen op allerlei terreinen, worden vakgebieden, onderzoekers en soms ook instellingen meegesleurd in polariserende discussies, ingeperkt in hun vrijheid en soms ook fysiek bedreigd (Eimers et al., 2023).



RISICO'S EN
DREIGINGEN
VOOR HET HO:
DRIE
VOORSTELBARE
TOEKOMSTEN

4 RISICO'S EN DREIGINGEN VOOR HET HO: DRIE VOORSTELBARE TOEKOMSTEN

Hieronder volgen drie toekomstverkenningen (scenario's) waarin zichtbaar wordt gemaakt hoe risico's en dreigingen voor het hoger onderwijs zich de komende jaren zouden kunnen gaan manifesteren. Deze toekomstverkenningen zijn nadrukkelijk geen voorspellingen (*forecast*) maar voorstellingen (*foresight*) van voorstelbare toekomsten. Daarbij ligt de focus op belangrijke trends en ontwikkelingen zoals benoemd in hoofdstuk 2 en 3. Tevens gaat de aandacht uit naar de onderlinge verbonden- en verwevenheid tussen verschillende (toekomstige) risico's en dreigingen. Na elk scenario wordt een korte duiding gegeven.



SAMENVATTING SCENARIO 1

Een handvol handige hackers

- **Scenario:** Nadat een hoger onderwijsinstelling weigert zich uit te spreken over standpunten aangaande klimaatverandering en migratieproblematiek, neemt een handjevol *hacktivist*en het heft in eigen handen en zorgt er met verschillende (digitale) acties uiteindelijk voor dat het college van bestuur zich genoodzaakt ziet om af te treden.
- **Analyse:** Door toegenomen polarisatie en (geo) politisering zullen steeds vaker (h)ac(k)tivistische activiteiten zich binnen HO-instellingen gaan afspelen – wat grote impact kan genereren op sociale, fysieke én informatieveiligheid. Dit betekent dat instellingen moeten investeren in onder meer (cyber)weerbaarheid.

SCENARIO 1

Een handvol handige hackers

(H)ac(k)tivisme in een modern jasje

Context: Het is voorjaar 2025 en de geopolitieke spanningen in de wereld en de sociaal-maatschappelijke spanningen zijn allesbehalve afgenomen. De oorlog in Radestan en de desastreuze gevolgen van de mede door klimaatverandering veroorzaakte overstromingen in Balendië slepen voort. Migratiestromen via zowel de Europese oost- als zuidgrens bevinden zich op een ongekend hoog niveau. De thema's migratie en klimaatverandering zijn politiek en sociaalmaatschappelijk een steeds groter wordende splijtzwam geworden die de politiek en samenleving tot op het bot verdeelt.

De sociaalmaatschappelijke spanningen ten aanzien van vraagstukken rondom migratie en klimaatverandering komen binnen het hoger onderwijs steeds prominenter tot uiting. Groepen studenten staan lijnrecht tegenover elkaar en er ontstaat een angstcultuur onder veel docenten en studenten. Het merendeel van hen heeft 'besloten' om wijselijk de mond te houden (lees: zelfcensuur) om te voorkomen het mikpunt van kritiek of zelfs intimidatie te worden. Een groeiend

aantal studenten doet zijn beklag bij docenten en vertrouwenspersonen waarbij zij aangeven dat zij zich niet meer veilig voelen.

Het college van bestuur van Huygens Hoger Onderwijs komt tot de conclusie dat (re)actie van hun kant nodig is. Op het web en via de mail worden de studenten geïnformeerd dat het voor het bestuur van het allergrootste belang is dat een vrij en open debat over klimaatverandering en migratieproblematiek mogelijk blijft, dat het daarbij ook mag schuren – maar dat een veilige werk- en studeeromgeving daarbij gewaarborgd moet blijven. Dit bericht schiet bij een aantal studenten totaal in het verkeerde keelgat. Enkele tientallen van hen staan de volgende dag met protestborden voor de deur: ‘Spreek je uit’, ‘Klimaatontkenning is geen mening!’ en ‘Wegkijken is wegwezen!’

Een handjevol *tech-savvy* studenten is woedend over het gebrek aan actie van het bestuur en besluit dat zij zelf actie moeten ondernemen. De gedachte: ‘als het bestuur geen stelling durft in te nemen over zaken die door de wetenschap dubbel en dwars zijn bewezen, dan doen wij het wel voor ze’.

En dat is wat gebeurt. Het hek is van de dam en in rap-tempo volgen de ontwikkelingen elkaar op. Activisten nemen de website en de *socials* van Huygens HO over en plaatsen een pamflet waarin hun politieke boodschap ten aanzien van migratie en klimaatverandering

wordt overgebracht, evenals hun eis aan het bestuur om op te stappen. Ook is er sprake van *defacements*.⁷ Op zowel de LinkedIn-pagina als het twitteraccount van Huygens worden ook plagerige berichtjes geplaatst dat het bestuur er ook wel een beetje om vraagt om zo aangepakt te worden aangezien nog altijd dezelfde wachtwoorden gebruikt worden als jaren terug. De wachtwoorden lagen gewoon op de digitale straat, zo bleek. Vervolgens verschijnt een video online van een bekende hoogleraar c.q. eerste lector van Huygens waarin zij aangeeft dat het vandaag de dag niet meer kan dat een college van bestuur geen stelling durft in te nemen over de catastrofale gevolgen van klimaatverandering. Er zit niets anders op dan dat het bestuur aftreedt, stelt ze indringend vast. Het filmpje gaat viraal en wordt overgenomen door verscheidene mediakanalen. Een dag later blijkt het te gaan om een *deepfake*.⁸

De week erop wordt het wellicht nog gekker wanneer plots de smart boards in alle leslokalen overgenomen

⁷ Bij een defacement, ook soms bekend als een digitale bekladding van een website, verandert een aanvalleur de inhoud van bestaande webpagina's of plaatst nieuwe pagina's onder valse vlag (NCSC, 2015).

⁸ Een deepfake is beeld, geluid of ander materiaal dat geheel of gedeeltelijk is gefabriceerd of bestaand materiaal dat is gemanipuleerd met behulp van geavanceerde technische hulpmiddelen en dat niet of nauwelijks van echt te onderscheiden is (Van der Sloot, Wagenveld & Koops, 2021).

worden en de tekst ‘moderne Maagdenhuisbezetting’ in beeld verschijnt. Diezelfde dag beginnen ook de printers zich er mee te bemoeien en rolt de boodschap ‘Wegkijken is wegwezen: spreek je uit tegen klimaatontkenning!’ duizenden malen uit de printers. Tijdens een examen gaan plots de brandalarmen af wat een paniekerige ontruiming veroorzaakt, mede omdat er niet voldoende BHV'ers aanwezig zijn. Het blijft onduidelijk of het afgaan van het brandalarm toeval is of dat hier ook een kwade hand achter zat.

Richting het eind van de maand blijkt dat ook in het salarissysteem gerommeld is en de salarissen van sommige medewerkers stopgezet en van anderen juist flink verhoogd is. Als klap op de vuurpijl ontvangen alle Huygens-medewerkers een brief op de deurmat waarin ze gevraagd worden zich uit te spreken tegen het huidige college van bestuur.

In een spoedbijeenkomst trekt het college van bestuur de pijnlijke conclusie dat hun positie door de ongeregelde onhoudbaar is geworden en dat een nieuw college orde op zaken moet gaan stellen. Een paar (vooralsnog) anoniem gebleven studenten viert stilletjes feest. In de bestuurskamer, bij de koffieautomaat en in het fietsenhok van verscheidene HO-instellingen komen steeds twee vragen naar ter sprake: ‘Loont het nou echt om via (subversief) hacktivisme je politieke mening door te drukken?’ en ‘Wat mag je eigenlijk verwachten van een bestuur?’

Analyse

De in het scenario geschetste ontwikkelingen raken het hoger onderwijs op uiteenlopende manieren. Er is duidelijk impact op elk van de drie domeinen zoals vastgesteld door Platform IV-HO. Ten eerste is de sociale veiligheid in het geding omdat studenten, docenten en wetenschappers zich bedreigd voelen, wat bij sommige docenten en wetenschappers leidt tot zelfcensuur.⁹ Deze bedreiging is reëel, gezien docenten in het scenario het mikpunt worden van (des) informatiecampagnes en bovendien zelfs worden benaderd in hun eigen huis. Ook op het domein informatie-veiligheid is er impact, omdat de digitale integriteit aangetast wordt. Zo worden de sociale media van de hoger onderwijsinstelling gehackt en de smartboards overgenomen om daar activistische leuzen op weer te geven. Als laatste wordt de fysieke veiligheid zelfs aangetast, omdat het plots afgaan van het brandalarm zorgt voor een paniekerige ontruiming waarbij mogelijk mensen gewond kunnen raken.

Dit scenario staat symbool voor de toenemende spanningen die te voelen zijn in en rondom hoger onderwijsinstellingen. Gebeurtenissen die zich op het wereldtoneel afspelen, worden steeds vaker weerspie-

geld in de discussies en veiligheid rondom hoger onderwijsinstellingen. In dit scenario is gekozen voor de HO-instelling als een toneel voor uitingen van spanningen t.a.v. klimaatactivisme¹⁰ – echter had ook gekozen kunnen worden voor andere aanleidingen/onderwerpen zoals onvrede over het beleid van een instelling over thema's als privacy, grensoverschrijdend gedrag of samenwerkingen met bedrijven of landen.

Bovendien speelt het scenario in op de reeds zichtbare trend in de bredere maatschappij waarbij individuen een verhoogde intentie hebben om activiteiten uit te voeren om bepaalde standpunten kracht bij te zetten, maar ook een steeds groter wordende digitale capaciteit hebben om daad bij woord te voegen. De beschreven digitale activiteiten in het scenario worden vormgegeven door een handvol handige 'hackers' die zelf studeren aan desbetreffende onderwijsinstelling. Er zijn ook scenario's voorstelbaar waarin ook externen zich gaan mengen, bijvoorbeeld *copycats* (ook simpelweg voor de lol) of actieve steunverleners. Ook zou er steun kunnen ontstaan vanuit de (inter)nationale klimaatbeweging, of andersoortige activistische bewegingen. Het is zelfs voorstelbaar dat statelijke actoren, zoals bijvoorbeeld Rusland, misbruik maken

van dergelijke situaties om polarisatie te versterken. Terwijl het scenario zich afspeelt op slechts één HO-instelling, is er een reële kans dat dergelijke bewegingen/acties overslaan naar andere instellingen.

Hoger onderwijsinstellingen zullen aan deze thematiek aandacht moeten besteden – ook omdat de gevolgen van soortgelijke scenario's op veel vlakken de veiligheid nadelig kunnen beïnvloeden. In praktische termen betekent dat meer investeren in cyberweerbaarheid, onder andere door het aantrekken van meer IT-experts, het opleiden en regelmatig trainen van ICT- en andere relevante medewerkers in cyberveiligheid. Maar ook het creëren van een breder bewustzijn onder staf en studenten over cyberhygiëne. Daarnaast blijft het natuurlijk van belang om ook de meer gangbare risico's, zoals de afwezigheid van BHV'ers, te verminderen door te zorgen voor een goede bezettingsgraad.

⁹ Hier is momenteel al in beperkte mate sprake van (Technopolis group, 2023, pp. 72-73), maar door de toenemende polarisatie en politisering in en van het onderwijs zal dit waarschijnlijk enkel toenemen.

¹⁰ Onder andere zijn er bij de Universiteit Utrecht, de Erasmus Universiteit van Rotterdam, de Hogeschool Van Hall Larenstein, TU Delft en de Universiteit van Amsterdam al klimaatprotesten geweest (Universiteit van Amsterdam, 2023).

SAMENVATTING SCENARIO 2

Waar een wil is, is een (om)weg

- **Scenario:** Nadat verscheidene maatregelen zijn getroffen gericht tegen spionage en beïnvloeding vanuit het buitenland, gaan HO-instellingen ervan uit dat zij hierdoor niet meer kunnen worden geraakt. Echter worden altijd andere (digitale) wegen gezocht – waardoor buitenlandse actoren alsnog hun doelen kunnen bereiken.
- **Analyse:** Er bestaan grote botsende belangen tussen de gevaren van spionage en beïnvloeding enerzijds en zaken als academische vrijheid en het aantrekken van talent anderzijds. Behalve dat het van belang is om, per instelling, een gezonde balans hierin te vinden, moeten alle instellingen het adagium *assume breach* in gedachten houden. Omdat er tevens veelal sprake is van een waterbedeffect moeten niet alleen maatregelen worden genomen die enkel de *kans* maar ook de *impact* van scenario's als deze verkleinen.

SCENARIO 2

Waar een wil is, is een (om)weg

Constante uitdagingen op het gebied van spionage, kennisveiligheid en heimelijke beïnvloeding.

Context: Het is 2026 en er zijn in Nederland de afgelopen paar jaar goede stappen gezet op het gebied van kennisveiligheid. Zo zijn zowel de wet Screening Kennisveiligheid als de wet Uitbreiding Strafbaarheid Spionageactiviteiten in 2025 in werking getreden. HO-instellingen voeren bovendien periodieke zelfevaluaties uit over hun kennisveiligheidsbeleid. Nadat de AIVD een ambtsbericht heeft uitgebracht worden de visa van twee Vylmeense studenten en twee Vylmeense onderzoeksassistenten nietig verklaard. De twee studenten hebben evident directe banden met Vylmeense militaire onderzoekscentra. De onderzoeksassistenten worden beiden opgepakt op verdenking van spionage. Eén van hen is werkzaam in een laboratorium van Hogeschool Baruch. De ander is werkzaam op aan de Spinoza Universiteit en geeft les bij de opleiding *Vylmenian Studies*.

Uit de rechtszaken komt naar voren dat beide onderzoeksassistenten waarschijnlijk jarenlang spioneerden voor de Vylmeense inlichtingendienst en hun instructies via hun ambassade ontvingen. In de media verschijnen berichten dat de diverse meldingen over de twee docenten niet adequaat opgepakt zouden zijn door beide hoger onderwijsinstellingen. Nederland verklaart vanwege het spionageschandaal een Vylmeense diplomaat tot *persona non grata* en Vylmenië spiegelt door ook een Nederlandse diplomaat het land uit te zetten. De relaties tussen Vylmenië en Nederland, die al gespannen waren, verslechteren.

Een aantal jaar later wordt in het jaarrapport 2028 van de AIVD, net als in eerdere jaarrapporten, gewaarschuwd dat de dreiging uitgaande van spionage en beïnvloeding door Vylmenië, Dalan en Interië van ernstige aard is. Daarbij wordt ook expliciet de dreiging vanuit deze landen richting Nederlandse bedrijven, kennisinstellingen en wetenschappers genoemd. Zo wordt gesteld dat zij 'het doelwit zijn van zowel legitieme als illegitieme middelen'. Deze waarschuwingen krijgen weinig opvolging vanuit HO-instellingen. Naar hun mening is de dreiging, mede door de eerder getroffen maatregelen, al grotendeels afgewend. Bovendien zijn er geen incidenten geweest in de afgelopen twee jaar.

In die twee jaar tijd zijn echter wel de tekorten van talentvolle (bèta-)studenten en -onderzoekers, verder opgelopen. Deze zijn nodig om de kennis en concurrentiepositie van Nederland te behouden, en idealiter zelfs te vergroten. Verder bestaat groot ongemak over het feit dat Nederlandse kennisinstellingen steeds vaker beticht worden van discriminatoire handelingen die de (academische) vrijheden in zouden perken.

De Vylmeense inlichtingendienst heeft zich tegelijkertijd geenszins af laten schrikken door de genomen maatregelen en is direct na de Nederlandse acties van twee jaar geleden aan de slag gegaan om nieuwe bronnen aan te boren. Waar een wil is, is een (om)weg. Een Nederlandse docent die al jarenlang succesvol samenwerkt met wetenschappers in Vylmenie wordt gerekruteerd om toegang te krijgen tot de onderzoeksresultaten van het bio-tech laboratorium van de Hogeschool Baruch. De docent had formeel geen toegang, maar kon desondanks met relatieve eenvoud een usb-stick met malware in een afgeschermd laboratoriumcomputer plaatsen. Ook weet de aan de Vylmeense inlichtingendienst gelieerde hackersgroep PROTHESIUM uiteindelijk toegang te krijgen tot bijna alle informatie op de interne schijven van een dozijn HO-instellingen. Deze toegang verkregen zij door via de mail te reageren op opengestelde vacatures. Wanneer een HR-medewerker de bijlage genaamd 'CV' opende, werd op de achtergrond het systeem geïnfecteerd. Zowel onderzoeksresultaten als ook persoonsgegevens worden

op deze manier op grote schaal binnengehaald. Beide heimelijke acties blijven onder de radar.

Deze informatie wordt niet alleen voor spionage- maar ook voor beïnvloedingsdoeleinden ingezet. De Vylmeense dienst heeft weet van de inhoud van een nog te publiceren kritisch onderzoek over de mensenrechtensituatie in Vylmenië, wat is uitgevoerd door onderzoekers verbonden aan de opleiding *Vylmenian Studies*. Tijdens een receptie ter gelegenheid van de Vylmeense nationale dag op de ambassade wordt één van de onderzoekers aangesproken door twee individuen die zich voorstellen als journalisten. Zij vertellen uitgebreid over hun *fact finding mission* waaruit blijkt dat Vylmenië goede stappen heeft gezet op het gebied van vrijheid van meningsuiting.

Een paar dagen later nemen dezelfde journalisten contact op met de onderzoeker, en nodigen haar uit om nog eens verder te praten over hun gedeelde interesse in de mensenrechtensituatie in Vylmenië onder het genot van een - natuurlijk door hen betaalde - chique lunch. Tijdens de lunch stellen de zogenaamde journalisten dat het fijn is om samen met een 'eerlijke en onbevooroordeelde' onderzoeker te spreken, en nodigen ze de onderzoeker uit voor een event met vooraanstaande Vylmeense gasten.

De onderzoeker vertrouwt de situatie niet en maakt melding van de gebeurtenissen bij haar onderwijs-

instelling en plaatst ook op X haar zorgen. Na deze (openlijke) bekendmaking melden meer medewerkers zich met zorgen dat er ook bij hen mogelijk sprake is geweest van ongewenste beïnvloeding.

Analyse

In het scenario is sprake van gebrek aan alertheid op het gebied van cyberveiligheid. Risico's en dreigingen op het gebied van spionage- en beïnvloeding door statelijke actoren zijn hoog en vereisen constante aandacht en actie. Tegelijkertijd kunnen deze acties ook zeker botsen en schuren met andere belangen op het gebied van academische vrijheid, autonomie van hoger onderwijsinstellingen, openheid en het aantrekken van talent (d'Hooghe & Martin, 2024). Dit vereist een ingewikkelde maar belangrijke balanceer-act in het hoger onderwijs en van de overheid (AWTI, 2022). Er is bovendien sprake van een waterbedeffect. Door acties te ondernemen tegen een bestaande dreiging (in dit geval buitenlandse studenten en onderzoekers) verplaatst de dreiging zich naar elders (Nederlandse docent). Actoren kiezen daarbij vaak de weg van de minste weerstand. Het is mede om die reden inzichtelijk om uit te gaan van het adagium *assume breach*¹¹ waar het gaat om (digitale) spionage en beïnvloeding

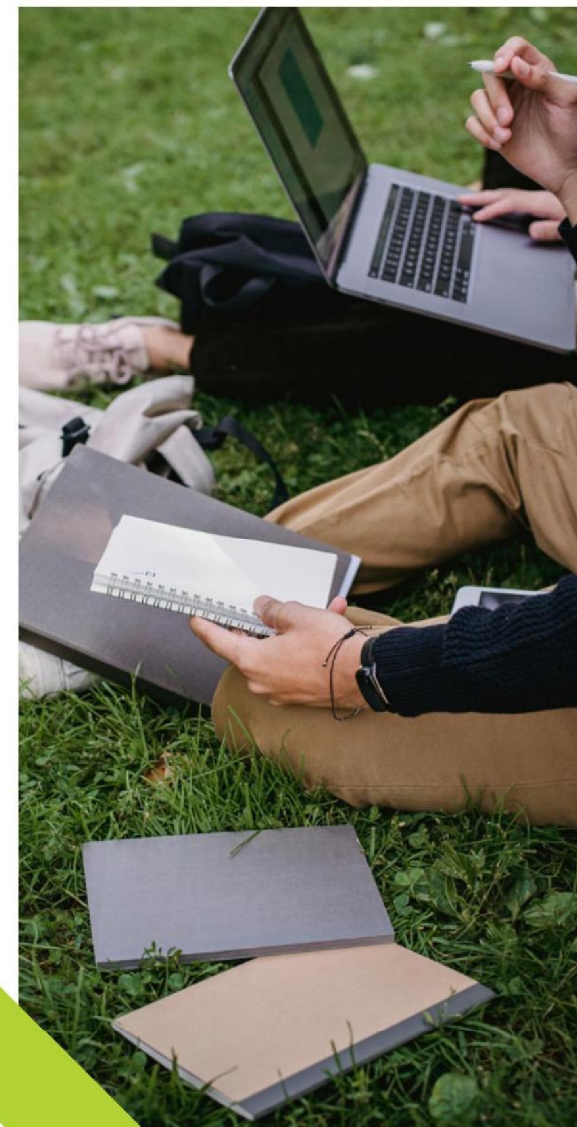
¹¹ *Assume breach* is een principe in de informatiebeveiliging dat inhoudt dat organisaties ervan uitgaan dat ze al zijn geschonden of dat ze in de toekomst zullen worden geschonden door kwaadwillende actoren.

door statelijke actoren. Als zij willen binnenkomen dan zullen ze linksom of rechtsom een heel eind kunnen komen.

Ook laat het scenario zien dat ‘positieve’ gevolgen van een maatregel op één van de thema's (kennisveiligheid) negatieve gevolgen kan hebben op zowel een ander aspect binnen hetzelfde thema als op andere thema's en overwegingen (sociale veiligheid en kennispositie). Dit is in het verleden ook op andere vlakken naar voren gekomen, zoals met maatregelen op het gebied van privacy (AVG), die vervolgens voor problemen zoals stroperige besluitvorming omtrent veiligheid zorgden. In de toekomst zou dit ook kunnen gebeuren op vlakken zoals bijvoorbeeld rondom nieuwe regelgeving over AI.

Het ingewikkelde van de geschetste problematiek is dat een deel van de dreiging zich onder de radar bevindt van desbetreffende onderwijsinstelling. Dat betekent echter niet dat er geen (grote) impact is of kan zijn. Onderzoeksresultaten en persoonsgegevens vloeien op grote schaal weg in dit scenario, hetgeen respectievelijk de kennispositie en de sociale veiligheid van medewerkers ondermijnt. Daarbij rijst de vraag of dit te wijten is aan onvoldoende beveiligde computersystemen en/of onvoldoende monitoring en afscherming van dataopslag – alsook in hoeverre maatregelen voor *insider threat* genomen zijn.

Een constant evaluerend pakket aan maatregelen zal daarom altijd nodig blijven om met dergelijke risico's en dreigingen om te gaan. Enerzijds om de kans op inbreuk te verkleinen en anderzijds om de impact te verkleinen wanneer er sprake is van inbreuk. Veiligheidsmaatregelen zijn in die zin nooit ‘af’. Uitwisseling van informatie en *best practices* tussen zowel Nederlandse als internationale HO-instellingen, alsook samenwerking en informatie-uitwisseling met Nederlandse veiligheidsinstanties vormen hiervan een belangrijk onderdeel.



SAMENVATTING SCENARIO 3

Soeverein in eigen brein

- **Scenario:** Door een combinatie van snelle technologische ontwikkelingen, een krappe arbeidsmarkt, politisering van het onderwijs en polarisatie neemt het aantal alternatieve vormen van educatie toe – waardoor de bestaanszekerheid van Nederlandse HO-instellingen mogelijk in het gedrang komt.
- **Analyse:** Flexibiliteit van hoger onderwijsinstellingen is nodig om het hoofd te kunnen blijven bieden aan grote veranderingen in de maatschappij en het HO-landschap. Zo zullen instellingen consequent moeten innoveren – op zowel technologisch als maatschappelijk gebied.

SCENARIO 3

Soeverein in eigen brein

Toenemende concurrentie voor en politisering van het (Hoger) Onderwijs

Context: Al geruime tijd groeit het aantal studenten die een opleiding aan het hoger onderwijs genieten gestaag en is in het laatste decennium het aantal hoogopgeleiden enorm omhooggeschoten (zie grafiek 1).¹²

Mede door de enorme stijging in aantal studenten zijn er grote knelpunten ontstaan met betrekking tot lesruimtes en de kwaliteit van onderwijs. Zo wordt noodgedwongen de keuze gemaakt om steeds meer hoorcolleges in plaats van werkgroepen te geven, waardoor studenten steeds minder contact hebben met de docenten en onderling. Ook worden steeds meer colleges online gegeven. Dit versterkt de voorgaande trend van de vermindering van contact tussen studenten onderling en met docenten.

In 2032 vragen steeds meer jongeren alsook bedrijven zich af wat nog de meerwaarde is van het volgen van een opleiding aan het hoger onderwijs. Het behalen van een diploma staat bij steeds meer vacatures niet meer als vereiste opgegeven. Spottend wordt door sommigen gezegd dat iedereen, met een beetje hulp van *FlatTPG* en vergelijkbare technologieën, met twee vingers in de neus een HO-diploma kan halen. Doordat de technologische ontwikkelingen zich de afgelopen jaren zo snel hebben opgevolgd, staan hogescholen en universiteiten voor enorme uitdagingen wat betreft innovatie. De bureaucratische manier van besluitvorming binnen deze instituties helpt daarbij niet. Tegelijkertijd schieten alternatieve vormen van educatie, die slim inspelen op de snelle ontwikkelingen, als paddenstoelen uit de grond. De meeste HO-instellingen voelen zich vooralsnog niet bedreigd hierdoor – de aanmeldingen zijn immers hoger dan ooit tevoren.

Sinds kort neemt echter het aantal jongeren dat besluit na de middelbare school niet op de ouderwetse manier verder te studeren toe. Liever gaan zij meteen de arbeidsmarkt op. Talentvolle scholieren kunnen vrijwel gelijk geld verdienen door bij een commercieel bedrijf aan de slag te gaan. Ze krijgen 'on the job training' of gaan traineeships aan met bedrijven die, mede vanwege een schaarse arbeidsmarkt, hunkeren naar talent. Ze zetten financiële en andersoortige prikkels in om talent aan zich te binden. Het Nederlandse hoger onderwijs ondervindt daarnaast ook groeiende

¹² Cijfers van 2013 en 2021 zijn overgenomen uit een CBS-rapport (van der Mooren & de Vries, 2022). Enkel de cijfers uit 2032 zijn fictief.

competitie uit het buitenland. *Startups, unicorns* en *Big-tech* bieden soms een nog aantrekkelijker alternatief dan de Nederlandse bedrijven al doen. Daarnaast bieden landen, zoals de Verenigde Staten van Vespucci, Golfstaat Habadja en de semi-onafhankelijke stadstaat Orang, zeer aantrekkelijke beurzen aan. Niet verrassend lopen studentenaantallen terug en een tijd later beginnen Nederlandse HO-instellingen dan ook stap voor stap weg te zakken in de wereldwijde ranglijsten.

Er is bovendien sprake van een groeiend aantal studenten dat halverwege zijn of haar opleiding afhaakt. Deels vanwege de krappe arbeidsmarkt en de legio arbeidskansen die er zijn, deels ook omdat zij de voorkeur geven aan een opleiding via nieuwe flexibele en goedkopere *online education platforms*. Met generatieve AI is het relatief gemakkelijk om een gepersonaliseerd onderwijsprogramma samen te stellen. Individuen kunnen dit zelf doen zonder enige technische kennis, maar betere varianten zijn ook commercieel beschikbaar. Het bedrijf dat het grootste aandeel heeft op deze markt is *Bigtech*-bedrijf Valdivia, die AI gebruikt om zelfs simulatie-games te maken waarin je één-op-één les krijgt van een ‘hoogleraar’. Door een tekort aan docenten wijken ook HO-instellingen steeds vaker naar dergelijke technieken uit, maar dit vertaalt zich niet in lagere collegegelden.

Ondertussen groeit het beeld dat HO-instellingen nog altijd wetenschappelijke objectiviteit prediken maar

dat daar in de praktijk weinig (meer) van terecht komt. Volgens de publieke opinie zijn universiteiten en hogescholen steeds gekleurder geworden. Waar voorheen de wetenschap als min-of-meer waardenvrij werd bestempeld is dat niet meer het geval. Zo kiezen rechtsgeoriënteerde individuen voor Hogeschool Boerhaave en linksgeoriënteerde individuen voor Hogeschool Grotius, omdat deze beter passen bij hun (politieke) wereldbeeld. Bewust of onbewust versterken de gebruikte technologieën van Valdivia deze trend, en krijgen studenten van verschillende scholen een aangepast onderwijsprogramma – ondanks dat dezelfde onderwerpen behandeld worden in vergelijkbare studies. Vol trots plaatsen steeds meer individuen dan ook op hun LinkedIn profielen dat ze ‘autodidact’ zijn en bewust de keuze hebben gemaakt om niet zo’n achterhaald en gepolitiseerd diploma te halen bij een ‘hogere’ onderwijsinstelling.

De afgelopen jaren is niet alleen de groep mensen die zichzelf trots autodidact noemt gegroeid, maar ook het aantal zelfbenoemde soevereinen.¹³ Zij hekelen de elite, waarvan de mainstream media en het hogere onderwijs deel uitmaken, en baseren hun kennis op een select aantal bronnen die niet onder invloed

¹³ Er zijn in Nederland naar schatting al ten minste enkele tienduizenden personen die in meer of mindere mate dit gedachtegoed aanhangen. De verwachting is dat deze beweging verder zal groeien (AIVD, Nationale Politie, NCTV, 2024, p. 19).

staan van deze ‘autoriteiten’. Onder hen bestaat ook een groeiende aversie tegen door de elite opgelegde inperkingen van privacy en vrijheden. Binnen deze beweging ontstaat het idee om – naast lager en middelbaar onderwijs – ook zelf hoger onderwijs aan te gaan bieden aan de leden van hun gemeenschap. Onder de hashtag #Soeverein-in-eigen-brein wordt online geld ingezameld om dit op te gaan zetten. Binnen *no-time* opent ‘De Autonome School’ zijn deuren.

Analyse

Technologische en sociaalmaatschappelijke ontwikkelingen hebben grote impact op het hoger onderwijs, zoals ook in dit scenario naar voren komt. Waar de eerste twee scenario’s zich toespitsen op een nauwere definitie van veiligheid en de middellange-termijn, speelt dit scenario zich af op de lange termijn en binnen een brede definitie van veiligheid. Ondanks het feit dat dit scenario zich niet op elk punt direct laat vertalen in concrete veiligheidsrisico’s en dreigingen, is het van belang om op dergelijke scenario’s te reflecteren om zo beter in te kunnen spelen op de lange termijn effecten van nieuwe ontwikkelingen.

Het hoger onderwijs zal waarschijnlijk in toenemende mate te maken krijgen met risico’s die voorkomen uit concurrerende onderwijsvormen. Deze kunnen geleidelijk ontstaan, maar kunnen zich juist ook snel ontwikkelen. Zowel commerciële bedrijven, andere landen, alsook individuen die handig gebruik maken

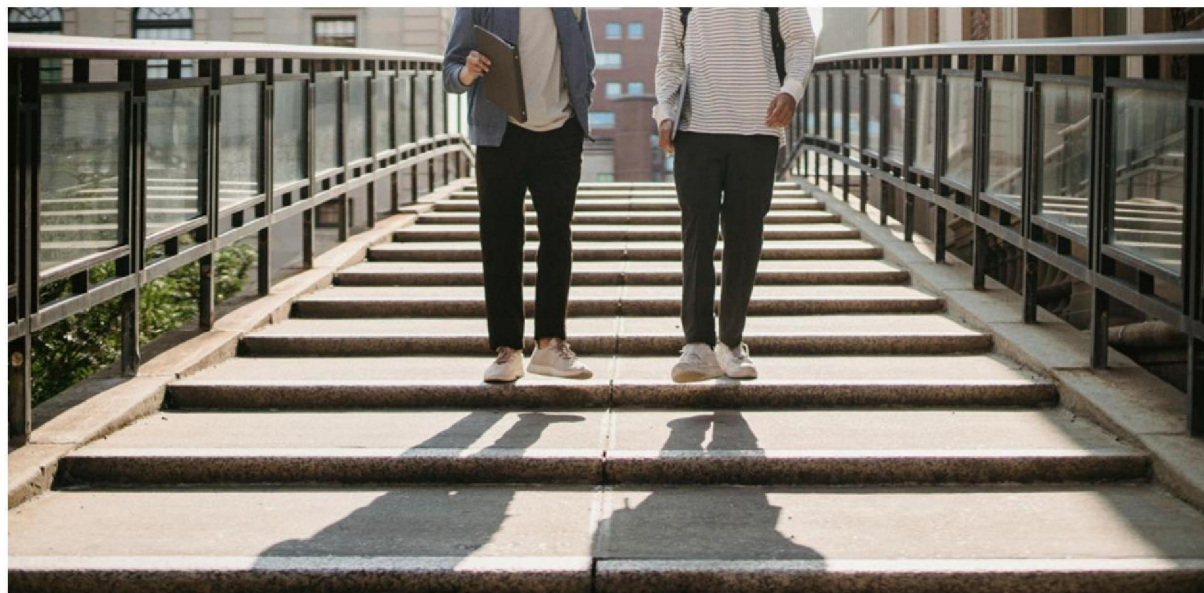
van nieuwe technologieën kunnen risico's voor het hoger onderwijs genereren. Ook de toenemende mobiliteit van (talentvolle) studenten en academici kunnen risico's en dreigingen voor het Nederlandse hoger onderwijs opleveren. Hierbij geldt dat deze met name ontstaan wanneer het hoger onderwijs niet voldoende in staat zal zijn om nieuwe kansen tot eigen voordeel aan te wenden.

Het scenario staat verder symbool voor het risico dat het hoger onderwijs verder gepolitiseerd raakt. De opkomst van nieuwe onderwijsinstellingen, zoals bijvoorbeeld 'De Autonome School', biedt alternatieve onderwijsbenaderingen aan wat de diversiteit van het onderwijslandschap vergroot. Dit kan echter ook de polarisatie/fragmentatie (binnen Nederland) versterken. Bovendien is de kans aanwezig dat groeperingen (of algoritmes) zich op mis- of desinformatie kunnen baseren en/of deze verder verspreiden.

De politisering van onderwijsinstellingen en de groeiende nadruk op specifieke wereldbeelden symboliseren de toenemende polarisatie binnen de samenleving. Het onderstreept de uitdagingen van het behouden van neutraliteit en objectiviteit in het onderwijs in een tijdperk van gepolariseerde opvattingen en ideologieën – en stelt de vraag in hoeverre dit überhaupt in de verdere toekomst nog mogelijk is.

De opkomende interesse in alternatieve leertrajecten en in gepersonaliseerd leren symboliseert ook de groeiende behoefte aan flexibiliteit en individualiteit in het onderwijs. Mensen zoeken steeds vaker naar manieren om hun vaardigheden en kennis op maat te ontwikkelen, om te voldoen aan de eisen van een snel veranderende arbeidsmarkt. De rol van technologie in dit scenario, met name Generatieve AI, in het leveren van gepersonaliseerd leren symboliseert de impact van technologische vooruitgang op het onderwijs. Het wijst op de mogelijkheden en uitdagingen van het integreren van nieuwe technologieën in het onderwijs-

proces. Hierbij wordt het risico op gekleurde algoritmes benoemd, omdat dit de eerdergenoemde trends van politisering en polarisatie mogelijk kan versterken. Het is dan ook belangrijk dat onderwijsinstellingen kunnen anticiperen, reageren en zich aan kunnen passen aan een snel veranderende wereld met snel veranderende benodigde vaardigheden van studenten. Voorzichtige en meer sluimerende ontwikkelingen kunnen zich door een samenloop van omstandigheden verder ontwikkelen naar een situatie waarin de prominente mondiale positie van het Nederlands hoger onderwijs rap verloren raakt.



5 CONCLUSIES

Het Risico- en Dreigingsbeeld Hoger Onderwijs 2024 biedt een uitgebreid inzicht in de complexe uitdagingen waarmee instellingen worden geconfronteerd. De rode draad is de toenemende verwevenheid van verschillende ontwikkelingen: tussen risico's en dreigingen in de maatschappij en in het hoger onderwijs, en tussen de verscheidene risico's en dreigingen binnen het hoger onderwijs onderling. Niettemin springen enkele thema's in het oog, vanwege hun groeiende omvang en impact:

- de brede impact van geopolitieke ontwikkelingen en maatschappelijke problemen op het functioneren van HO-instellingen;
- de toename van activisme, zorgwekkend gedrag en radicalisering die grote risico's kunnen opleveren voor fysieke en sociale veiligheid;
- de uitdagingen die snelle technologische ontwikkelingen met zich meebrengen;
- toename in ongewenste activiteiten van statelijke en criminele actoren;
- de groeiende beknotting van academische vrijheid;
- de voortdurende zorgen rondom (seksueel) grensoverschrijdend gedrag, waarvan de meldingen sterk zijn toegenomen.

Deze en eerdergenoemde risico's zullen zich op verschillende manieren en in verschillende mate binnen de diverse hoger onderwijsinstellingen in Nederland manifesteren. We kennen immers een enorm divers HO-landschap – waar omvang, studentenpopulatie,

ligging en activiteiten sterk uiteenlopen. Maar voor allen geldt dat een **integrale aanpak** en een **goed ontwikkeld risicomanagement** essentieel is. De onzekerheid rondom de impact van nieuwe ontwikkelingen, zoals opkomende technologieën, noopt tot een **toekomstgerichte en wendbare aanpak**. Daarnaast vragen de urgentie van sommige risico's en dreigingen, en/of de lange adem die beleidsontwikkeling en -implementatie vergen, om **actie op de korte termijn**: er moet *nu* proactief wat mee gedaan worden.

Kijkend naar de toekomst zijn het **vergroten van cyberweerbaarheid** en het **versterken van risicomanagement** belangrijke speerpunten van beleid. Daarbij zal men moeten uitgaan van het adagium ***assume breach***, zodat niet enkel de kans op een ongewenste gebeurtenis wordt verkleind – maar ook de potentiële impact ervan mocht er onverhoopt toch een dergelijke gebeurtenis plaatsvinden. Voor deze maatregelen zal meer mankracht en expertise nodig zijn – maar ook een groeiend bewustzijn en aanpassingsvermogen onder het bestuur, medewerkers en studenten.

Alleen door gezamenlijke inspanningen en een voortdurende toewijding aan veiligheid en veerkracht kunnen hoger onderwijsinstellingen een veilige en stimulerende leeromgeving bieden voor studenten, wetenschappers en medewerkers – zowel nu als in de (verre) toekomst.

BIJLAGEN

BIJLAGE 1 METHODOLOGISCHE VERANTWOORDING

Voor dit onderzoek zijn verschillende methoden gebruikt om inzicht te verkrijgen in de risico's en dreigingen die zich nu of binnen de komende jaren (focus op de komende vijf jaar) kunnen ontwikkelen en/of voordoen bij HO-instellingen. Daarbij wordt voortgebouwd op het voorgaande Risico- en Dreigingsbeeld en ligt de focus op trends, ontwikkelingen en risico's en dreigingen die nieuw zijn (IVHO & COT, 2021). Voor dit onderzoek is gebruik gemaakt van openbronnenonderzoek, expertinterviews, *strategic foresight*-methodieken (*horizon scanning* en *scenario-building*) en zijn meerdere dialoogtafels georganiseerd met stakeholders uit een diverse groep hoger onderwijsinstellingen en gelieerde organisaties.

Het onderzoek neemt als basis de drie domeinen en negen thema's die door het Platform Integrale Veiligheid Hoger Onderwijs worden gehanteerd en waarbinnen risico's en dreigingen zich (kunnen gaan) manifesteren.¹⁴ De drie domeinen zijn:

1. Sociale veiligheid;
2. Informatieveiligheid;
3. Fysieke veiligheid.

De geïdentificeerde thema's, welk binnen één of meerdere van bovenstaande domeinen zich kunnen bevin-

den zijn: (1) Integriteit, (2) Arbo en milieu, (3) Sociale veiligheid, (4) Zorgwekkend gedrag en radicalisering, (5) Gebouwveiligheid, beveiliging en BHV, (6) Cyberveiligheid, (7) Kennisveiligheid en ongewenste beïnvloeding, (8) Internationalisering en (9) Privacy.

Open bronnenonderzoek en expertinterviews

In de beginfase van het onderzoek is een openbronnenonderzoek uitgevoerd om breed inzicht te verkrijgen in de bestaande kennis en onderzoeksbevindingen op het gebied van risico's en dreigingen voor HO-instellingen, alsook (inter)nationale veiligheid in de bredere zin. De focus van het openbronnenonderzoek lag op de verschillende relevante beleidsdocumenten, onderzoeksrapporten en nieuwsberichten. Deze zijn geïdentificeerd via gangbare zoekmachines en bibliotheekcatalogi, onder de voorwaarde dat ze gepubliceerd zijn na het vorige Risico- en Dreigingsbeeld van 2021 (IVHO & COT, 2021). Vervolgens werden de verzamelde bronnen extensief doorgenomen om de relevantie te kunnen beoordelen.

Daarnaast zijn verschillende experts geïnterviewd, welke onder meer werkzaam zijn bij het Ministerie van Onderwijs en Cultuur, het kennisveiligheidsloket, de NCTV en de AIVD. De semigestructureerde interviews hebben nieuwe en aanvullende inzichten verschaft op de (toekomstige) risico's en dreigingen welke eerder geïdentificeerd zijn uit open bronnen.

Horizonscan

Op basis van de input uit het openbronnenonderzoek en de expertinterviews is een horizonscan uitgevoerd. Dit is één van de methodieken binnen *strategic foresight*, waarbij systematisch verschillende bronnen worden gescand om vroege en/of zogenaamde zwakke signalen te herkennen van mogelijk belangrijke trends en ontwikkelingen. De focus van deze exercitie lag op de vooraf door SURF vastgestelde thema's. Om de verbondenheid tussen de onderwerpen mee te nemen werd op systematische wijze vastgelegd of de verzamelde signalen op één of meerdere thema's en domeinen van toepassing zijn.

Scenario building

Om toekomstige risico's en dreigingen inzichtelijk en voorstelbaar te maken zijn vervolgens scenario's opgesteld. Op basis van het open bronnenonderzoek, groepsgesprekken, interviews en de horizonscan zijn drie combinaties van thema's uitgekozen. Deze zijn vervolgens uitgewerkt in korte voorstelbare verhaallijnen, omdat de aan deze thema's gelieerde risico's en dreigingen mogelijk een grote(re) rol zullen spelen in de toekomst.

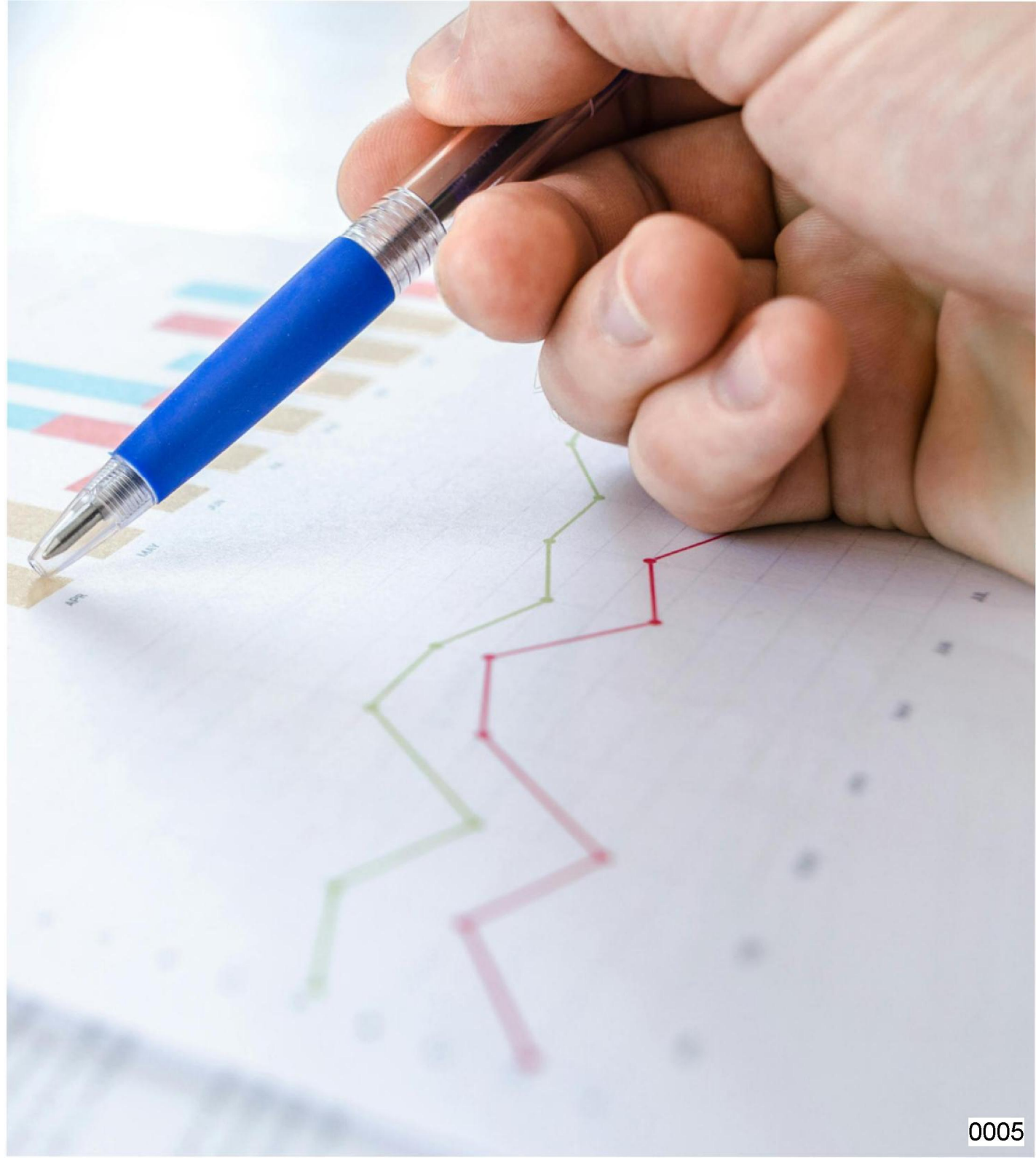
Om de scenario's systematisch uit te werken is gebruik gemaakt van een morfologische analyse. Deze geeft een schematisch overzicht van de relevante factoren, impact en actoren binnen een thema. Door verschillende combinaties hierbinnen uit te lichten kunnen

¹⁴ Voor definities van de drie domeinen en negen thema's zie hoofdstuk 2.

verschillende scenario's worden bedacht, met wisselende uitkomsten. De gebruikte bouwstenen voor de drie scenario's in hoofdstuk 2 zijn aan het einde van deze methodologische verantwoording toegevoegd.

Dialogotafels

Aanvullend zijn meerdere dialogotafels gehouden met stakeholders uit een diverse groep medewerkers van hoger onderwijsinstellingen, alsook gelieerde organisaties en experts. Tijdens de eerste dialogotafel lag de focus op nieuwe ontwikkelingen die praktijkdeskundigen uit het hoger onderwijs zelf onderkennen op de eerdergenoemde thema's. Hierbij speelden de factoren *kans*, *impact* van en bewustzijn over risico's en dreigingen een belangrijke rol. De tweede dialogotafel richtte zich voornamelijk op (mogelijke) *toekomstige* ontwikkelingen. Dit werd als input meegenomen in verschillende stadia van het onderzoeksproces.



MORFOLOGISCHE ANALYSE ALS BASIS VOOR DE SCENARIO'S

Scenario 1:
Een handjevol handige hackers

| DOMEIN | THEMA | ONDERWERPEN / ONTWIKKELINGEN | HANDELENDE ACTOR | DOEL | SOORT ACTIVITEIT | IMPACT OP |
|-----------------------|---------------------------------------------|------------------------------|-------------------------|---------------------------------------------|--------------------------|---------------------------|
| Fysieke veiligheid | Integriteit | Polarisatie | Nederlandse student(en) | Maatschappelijke verandering teweeg brengen | Demonstratie | Student(en) |
| Sociale veiligheid | Arbo en milieu | (Geo)politisering | | Aandacht voor standpunt krijgen | Hacktivism | Medewerker(s) |
| Informatie-veiligheid | Sociale veiligheid | Zelfcensuur | | Afdwingen besluit | Defacements | College van Bestuur |
| | Zorgwekkend gedrag en radicalisering | Activisme | | Persoon in kwaad daglicht zetten | Desinformatie (campagne) | Hoger onderwijsinstelling |
| | Gebouwveiligheid, BHV en Fysieke Veiligheid | Datalek(ken) | | Beschadigen imago | Intimidatie | Gebouw (veiligheid) |
| | Cyberveiligheid | Generatieve AI | | | Cancelen | |
| | Kennisveiligheid en ongewenste beïnvloeding | Bestuurlijke integriteit | | | | |
| | Internationalisering | Afwezige BHV'ers | | | | |
| | Privacy | | | | | |

Scenario 2:
Waar een wil is, is een (om)weg

| DOMEIN | THEMA | ONDERWERPEN / ONTWIKKELINGEN | HANDELENDE ACTOR | DOEL | SOORT ACTIVITEIT | IMPACT OP |
|-----------------------|---------------------------------------------|---------------------------------------|----------------------------|----------------------------------------|-------------------------|----------------------------|
| Fysieke veiligheid | Integriteit | Wetenschappelijke integriteit | Internationale student(en) | Verwerving kennis en technologie | Spionage | Student(en) |
| Sociale veiligheid | Arbo en milieu | Academische vrijheid | Nederlandse Docent(en) | Beïnvloeden onderzoeksresultaten | Digitale spionage | Medewerker(s) |
| Informatie-veiligheid | Sociale veiligheid | Discriminatie | Internationale Docent(en) | Steun verwerven voor land en/of beleid | Omkoping | Hoger onderwijs-instelling |
| | Zorgwekkend gedrag en radicalisering | (geo)politisering | Statelijke actor(en) | Beschermen eigen groep/identiteit | Ongewenste beïnvloeding | College van Bestuur |
| | Gebouwveiligheid, BHV en Fysieke Veiligheid | Datalek(ken) | | | Politieke drukmiddelen | Nationale Veiligheid |
| | Cyberveiligheid | Ongewenste kennisoverdracht | | | | |
| | Kennisveiligheid en ongewenste beïnvloeding | Economische veiligheid | | | | |
| | Internationalisering | Internationale samenwerkingsverbanden | | | | |
| | Privacy | Wet Screening Kennisveiligheid | | | | |
| | | Inkomende mobiliteit | | | | |

Scenario 3: Soeverein in eigen brein

| DOMEIN | THEMA | ONDERWERPEN / ONTWIKKELINGEN | HANDELENDE ACTOR | DOEL | SOORT ACTIVITEIT | IMPACT OP |
|-----------------------|---------------------------------------------------|-----------------------------------|-------------------------------------|--------------------------------------------------|-------------------------|--------------------------------|
| Fysieke veiligheid | Integriteit | Anti-institutioneel extremisme | Nederlandse student(en) | Maatschappelijke veran- dering teweeg brengen | Innovatie | Student(en) |
| Sociale veiligheid | Arbo en milieu | (geo)politisering | Internationale student(en) | Beschermen eigen groep/identiteit | Concurreren | Medewerker(s) |
| Informatie-veiligheid | Sociale veiligheid | Polarisatie | Extern persoon/ externe personen | Talent werven | Inspelen op polarisatie | Hoger onderwijs- instelling |
| | Zorgwekkend gedrag en radicalisering | Generatieve AI | Commerciële bedrijven | Beschermen eigen groep/identiteit | | Externen |
| | Gebouwveiligheid, BHV en Fysieke Veiligheid | Onderwijskwaliteit | Statelijke actor(en) | | | |
| | Cyberveiligheid | Ondermijning | | | | |
| | Kennisveiligheid en ongewenste beïnvloeding | Academische vrijheid | | | | |
| | Internationalisering | | | | | |
| | Privacy | | | | | |

BIJLAGE 2 BIBLIOGRAFIE

Aartsma, K., & Dijkman, M. E. (2024). Soevereiniteit en Beïnvloeding. In *Bijlagen Barsten en Blokken: Confrontatie en samenwerking in een wereld van wisselende coalities*.

Adviesraad voor Wetenschap, Technologie en Innovatie [AWTI]. (2022). *Kennis in Conflict Veiligheid en Vrijheid in Balans*.

Algemeen Dagblad [AD]. (2021, 9 december) Universiteit Leiden zet omstreden mensentellers uit om zorgen over privacy.

Algemene Inlichtingen en Veiligheidsdienst [AIVD], Militaire Inlichtingen- en Veiligheidsdienst [MIVD], & Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2022). *Dreigingsbeeld Statelijke Actoren 2*.

Algemene Inlichtingen en Veiligheidsdienst [AIVD]. (2023a). *Jaarverslag 2022*.

Algemene Inlichtingen en Veiligheidsdienst [AIVD]. (2023b). *Anti-Institutioneel Extremisme in Nederland: Een ernstige dreiging voor de democratische rechtsorde?* Algemene Inlichtingen en Veiligheidsdienst [AIVD]. (2024). *Jaarverslag 2023*.

Algemene Inlichtingen en Veiligheidsdienst [AIVD], Nationale Politie, & Nationaal Coördinator

Terrorismebestrijding en Veiligheid [NCTV]. (2024). *Met de rug naar de samenleving: Een analyse van de soevereinenbeweging in Nederland*.

Analistennetwerk Nationale Veiligheid [ANV]. (2022). *Rijksbrede risicoanalyse Nationale Veiligheid 2022*. Rijksoverheid.

Autoriteit Persoonsgegevens [AP]. (2020). *Datalekkenrapportage 2020*.

Autoriteit Persoonsgegevens [AP]. (2021). *Datalekkenrapportage 2021*.

Autoriteit Persoonsgegevens [AP]. (2022). *Datalekkenrapportage 2022*.

Autoriteit Persoonsgegevens [AP]. (2024). *Sectorbeeld Onderwijs 2021-2023*.

Baazil, D. (2024, 28 februari). Van de UvA naar de Zuidas. *De Groene Amsterdammer*.

Bekkers, F., Aartsma, K., & Sweijts, T. (2024, 13 februari). *Barsten en Blokken: Confrontatie en samenwerking in een wereld van wisselende coalities*.

Brink, A., & Van den Broek, A. (2022). *Sociale veiligheid in het hoger onderwijs*. ResearchNed.

Centraal Planbureau [CPB]. (2019). *Economische effecten van internationalisering in het hoger onderwijs en MBO*.

Commissie Stolker. (2022). *Eindrapport onderzoek Cross Cultural Human Rights Centre*. Vrije Universiteit Amsterdam.

College voor de Rechten van de Mens [CRM]. (2023, 17 oktober). Student niet gediscrimineerd door tentamensoftware Proctorio, maar VU had de klacht zorgvuldiger moeten behandelen.

Demiral, B., Koens, L., & Vennekens, A. (2024). *Internationalisering in perspectief: aantallen studenten, studiekeuzes en arbeidsmarkt*. Rathenau Instituut.

Dialogic, & Oberon. (2023). *Sectorbeeld kennisveiligheid universiteiten 2023*.

D'Hooghe, I., & Martin, X. (2024). *Dutch collaboration with PhD students sponsored by the Chinese Council*.

Dijkgraaf, R. (2022a, 13 juni). Internationalisering [Kamerbrief].

Dijkgraaf, R. (2022b, 23 december). Voortgang aanpak kennisveiligheid hoger onderwijs en wetenschap [Kamerbrief].

Dijkgraaf, R. (2023a, 21 april). Beheersing internationale studentenstromen in het hoger onderwijs [Kamerbrief].

Dijkgraaf, R. (2023b, 8 juni). Integrale aanpak sociale veiligheid in hoger onderwijs en wetenschap. [Kamerbrief].

Dijkgraaf, R. (2023c, 23 juni). Experiment flexstuden [Kamerbrief].

Dijkgraaf, R. (2023d, 16 oktober). Sectorbeeld kennisveiligheid universiteiten [Kamerbrief].

Dijkgraaf, R. (2023e, 21 december). Rectorenoverleg met betrekking tot wetenschappelijke integriteit en onafhankelijkheid [Kamerbrief].

Dijkgraaf, R., Adriaansens, M., & Yeşilgöz, D. (2022, 21 januari). Voorgang en vooruitblik aanpak kennisveiligheid hoger onderwijs en wetenschap. [Kamerbrief].

Eimers, T., den Boer, P., Leest, B., Raaijman, J., van der Vegt, J., Van den Berg, D., Vereijken, I., ...

Vloedveld, C. (2023). *Vandaag is het 2040: toekomstverkenning voor middelbaar beroepsonderwijs, hoger onderwijs en wetenschap*.

Favier, S., & Wijsenbeek B. (2023). *Factsheet internationale studenten*. Nuffic.

Feddes, A., Nickolson, L., & Doosje, B. (2015). Triggerfactoren in het radicaliseringsproces. Expertise-unit Sociale Stabiliteit.

Frankenhuis, G. (2023, 27 december). Dit is hoe geheimen criminele crystal meth-koks worden ontrafeld:

'Colombia is het Nederland van Zuid-Amerika'. *Dagblad van het Noorden*.

Games, A., & Okano-Heijmans, M. (2024). *Too late to act? Europe's quest for cloud sovereignty*. Clingendael.

Grapperhaus, F., Keijzer, M., & Van Engelshoven, I. (2020, 27 november). Kennisveiligheid hoger onderwijs en wetenschap. [Kamerbrief].

Giele, T. (2023, 25 november). Stop op buitenlandse studenten ramp voor hoger onderwijs Zeeland. *Provincie Zeeland Courant*.

Hagenauw, I., Holtman, J., & Maccow, D. (2023). *Tijdsbesteding HBO-Docenten*. Zestor.

Hamer, M. (2024, 24 januari). Advies over de aanpak van seksueel grensoverschrijdend gedrag en seksueel geweld in hoger onderwijs en wetenschap [Kamerbrief].

Hoger Onderwijs Persbureau. (2023, 16 januari). Bezetting bij UvA wegens banden met Shell.

Hu, K. (2023, 2 februari). ChatGPT sets record for fastest-growing user base – analyst note. *Reuters*.

Inspectie van het Onderwijs. (2021). *Binnen zonder kloppen-digitale weerbaarheid in het hoger onderwijs*.

Inspectie van het Onderwijs. (2022). *Sociale veiligheid in het hoger onderwijs factsheet*.

Inspectie van het Onderwijs. (2023). *Handvatten voor sturen op sociale veiligheid in het hoger onderwijs*.

Integrale Veiligheid Hoger Onderwijs [IVHO]. (z.d). *Handboek Integraal Veilig Internationaliseren*.

Integrale Veiligheid Hoger Onderwijs [IVHO]. (2018, 6 juni). *Integraal veiligheidsbeleid in het hoger onderwijs: Een intentieverklaring voor de sector en overheden*.

Integrale Veiligheid Hoger Onderwijs [IVHO], & Instituut voor Veiligheids- en Crisismanagement [COT]. (2021). *Risico- en Dreigingsbeeld hoger onderwijs 2021*.

Kammer, C., & Stefanovski, N. (2023, 22 september). Basisbeurs goed nieuws voor nieuwe studenten, maar lenen en bijnaam blijven noodzaak. *NRC*.

Kensenhuis, S. (2023, 20 november). Hogeschool waar docente opstapte vanwege racisme start minor discriminatie. *Algemeen Dagblad*.

Knight, J. (2008). An Internationalization Model: Meaning, rationales, approaches, and strategies. In P. Altbach (Red.), *Higher Education in Turmoil: The changing world of internationalization* (pp. 19-37). Rotterdam, Nederland: Sense Publishers.

Kommers, S, Peeters L., Staden, G., & Gaalen, A. (2021). *Internationaliseringsstrategieën in het hoger onderwijs*. Nuffic.

Koninklijke Nederlandse Akademie van Wetenschappen [KNAW]. (2021). *Academische Vrijheid in Nederland*.

Koninklijke Nederlandse Akademie van Wetenschappen [KNAW]. (2022). *Sociale veiligheid in de Nederlandse wetenschap: Van papier naar praktijk*.

Koninklijke Nederlandse Akademie van Wetenschappen [KNAW]. (2023). *Evaluatie Nederlandse gedragscode wetenschappelijke integriteit*.

Landelijk Orgaan Wetenschappelijke Integriteit [LOWI]. (z.d). *Adviezen van het Landelijk Orgaan Wetenschappelijke Integriteit*.

Landelijke stuurgroep toegankelijkheid en wachttijden ggz. (2023). *Regiomonitor toegankelijkheid en wachttijden eerste helft 2023*.

Militaire Inlichtingen- en Veiligheidsdienst [MIVD]. (2023). *Openbaar jaarverslag 2022 MIVD*.

Ministerie Binnenlandse Zaken en Koninkrijksrelaties [BZK], Ministerie van Onderwijs, Cultuur en Wetenschap [OCW], & Centraal Bureau voor de Statistiek [CBS]. (2022). *Kernrapport Werkonderzoek 2022*.

Ministerie van Economische Zaken en Klimaat [EZK]. (2024). *De Nationale Technologiestrategie*.

Ministerie van Financiën. (2019). *IBO: Internationalisering van het (hoger) onderwijs*.

Ministerie van Onderwijs, Cultuur en Wetenschap [OCW]. (2023a, 28 maart). Meer ademruimte voor studenten, docenten en onderzoekers: veel belangstelling voor slimmer inrichten van het collegejaar.

Ministerie van Onderwijs, Cultuur en Wetenschap [OCW]. (2023b, 21 juli). Besluit bestuurlijke boete Hogeschool Tio.

Ministerie van Onderwijs, Cultuur en Wetenschap [OCW]. (2023c, 21 december). Reactie Call for evidence Raadsaanbeveling kennisveiligheid [Kamerstuk].

Ministerie van Onderwijs, Cultuur en Wetenschap [OCW]. (2024, 8 maart). Loket Kennisveiligheid.

Muft, W. (z.d). Publieke waarden. *SURF*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2022a). *Dreigingsbeeld Terrorisme Nederland 56*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2022b) *Dreigingsbeeld Terrorisme Nederland 57*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2023a). *Dreigingsbeeld Terrorisme Nederland 58*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2023b). *Veiligheidsstrategie voor het Koninkrijk der Nederlanden*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2023c). *Dreigingsbeeld Terrorisme Nederland 59*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV]. (2023d). *Cyber Securitybeeld Nederland*. National Cyber Security Centrum [NCSC]. (2015). *Factsheet Help! Mijn website is beklad*.

Nederlands Instituut Publieke Veiligheid [NIPV]. (2022). *Toekomstverkenning brandweer 2022-2030*.

Nederlands Jeugdinstituut. (z.d.). *Wat is radicalisering?*

NOS. (2023a, 13 januari). Eerstejaars in Maastricht krijgen verplicht les over seksueel wangedrag.

NOS. (2023b, 6 mei). Saudische universiteit betaalde Nederlandse wetenschappers voor prestige.

NOS. (2023c, 9 december). Aantal buitenlandse studenten met Nederlandse studiebeurs sterk gestegen.

NOS. (2024a, 13 januari). Gaza-spanningen op universiteiten, in Leiden voelen studenten zich onveilig.

NOS. (2024, 24 januari). Advies: meer nodig voor aanpak seksueel wangedrag in hbo en wo.

Nuffic. (2023). *Toekomst van internationalisering in het mbo en ho: Een overzicht van Nuffic onderzoeken*.

Omroep West. (2023, 15 oktober). Brandweer zet in op betere brandveiligheid in studentenhuizen.

Onderwijsraad. (2022). *Inzet van intelligente technologie*.

Rathenau Instituut. (2022). *Naar hoogwaardig digitaal onderwijs*.

Rijksinstituut voor Volksgezondheid en Milieu [RIVM]. (2021). *Monitor Mentale Gezondheid en Middelengebruik van Studenten hoger onderwijs 2021*.

Rijksinstituut voor Volksgezondheid en Milieu [RIVM]. (2023). *Monitor Mentale Gezondheid en Middelengebruik van Studenten 2023*.

Rijksoverheid. (2023, 24 juli). *Aanpak extremisme en radicalisering in het onderwijs*.

RTL Nieuws. (2018, 1 december). Chemiestudenten geronseld door criminelen om te werken in xtc-labs.

RTL Nieuws. (2024, 10 april). Eén hack, grote gevolgen: gegevens 2,5 miljoen Nederlanders op straat.

ScienceGuide. (2023, 31 oktober). Geneeskundestudent van buiten Europa wordt in Nederland gediscrimineerd.

Slappendel-Henschen, A. (2022, 15 augustus). Vormen van internationalisering voor de student, docent en instelling. *Onderwijskennis*.

Slegers, S. [Host]. (2023). Vriend of Vijand. [Podcast]. Prospektor, Argos (HUMAN/VPRO), & NPO Radio 1.

Smaling, E. (2023, 13 oktober). 18 van 20 EUR-studenten terug uit Israël, 'alle studenten veilig'. *Erasmus Magazine*.

Smits, H., & Eikelenboom, S. (2024, 18 februari). Zuidas beslist mee over docenten en inhoud van universitair onderwijs. *Follow The Money*.

Spoor, B. (2023, 26 september). Privacy-volwassenheid TU/e krijgt een 1,3: dataprotectie niet op orde. *Cursor*.

Scientific Foresight Unit of the European Parliament Research Service [STOA]. (2024). *EP Academic Freedom Monitor 2023*. Europees Parlement.

SURF. (2023a). *Cyberdreigingsbeeld 2023: Onderwijs en onderzoek*.

SURF. (2023b). *Surf Tech Trends 2023*.

SURF. (2023c, 5 juli). *Privacyrisico's uit DPIA van 2023 Google Workspace for Education voldoende opgelost*.

SURF, & BDO. (2022). *Sectorrapportage 2022: Over security- en privacy-awareness in onderwijs en onderzoek*.

SURF, BDO, & The Hague University of Applied Sciences. (2023). *Sectorrapportage 2023: Over security en privacy awareness in onderwijs en onderzoek*.

Technopolis Group. (2023). *Onderzoek naar zelfcensuur in hoger onderwijs en wetenschap*.

Ten Have, M., Tuithof, M., Van Dorsselaer, S., Schouten, F., & De Graaf, R. (2022). *Trends NEMESIS: Trends naar demografie*.

Teunis, H. (2022, 20 oktober). Gegevens duizenden studenten TU Eindhoven gelekt bij hack. *RTL Nieuws*.

TNO. (2023, 26 oktober). Aantal thuiswerkuren sinds coronapandemie fors gestegen.

Transparency International Nederland. (2021). *Verkennd onderzoek educatie in ethiek en integriteit in het hoger onderwijs*.

Twigt, A. (2024, 19 januari). Afscheid MIVD laat generaal Swillens niet onberoerd. *Defensiekrant*.

Universiteit van Amsterdam. (2023, 16 mei). Protest Amsterdam Autonomous Coalition op Roeterseilandcampus.

Universiteiten van Nederland [UNL]. (2023). *Landelijk Model Klachtenregeling Wetenschappelijke Integriteit*.

Universiteiten van Nederland [UNL]. (2024a). Overzicht registratie nevenwerkzaamheden hoogleraren Nederlandse universiteiten.

Universiteiten van Nederland [UNL]. (2024b, 8 februari). Universiteiten nemen maatregelen om instroom internationale studenten te beheersen.

Universiteiten van Nederland [UNL]. (2024c, 2 april). Universiteiten maken werk van meer Nederlandstalige bachelors.

Universiteiten van Nederland [UNL], Koninklijke Nederlandse Akademie van Wetenschappen [KNAW], Vereniging Hogescholen [VH], NFU, TO federatie, Rijksoverheid, & NWO. (2022). *Nationale leidraad kennisveiligheid*.

Van der Mooren, F., & de Vries, R. (2022). *Steeds meer hoogopgeleiden in Nederland: wat voor beroep hebben ze?* Centraal Bureau voor de Statistiek [CBS].

Van der Sloot, B., Wagenveld, Y., & Koops, B. (2021). *Deepfakes: De juridische uitdagingen van een synthetische samenleving*.

Van der Torre, E., Tops, P., van Duin, M., & Jongepier, T. (2023). *Ondermijning in het Ommeland: Een analyse van (de gemeentelijke aanpak van) ondermijning in negen Groningse gemeenten*.

Van der Varst, L., Kaptein, N., Kuipers, F., & Dalmeijer, N. (2018). *Dreigingsbeeld Hoger onderwijs 2018*. IVHO.

Van der Veldt, M. (2023, 6 december). Students uncover security flaw: Backdoor TU Delft email traffic was wide open. *Delta*.

Van Dongen, M., & Dominicus, T. (2023, 16 januari). Bezetting gebouw door UvA-studenten beëindigd, 30 arrestaties. *Het Parool*.

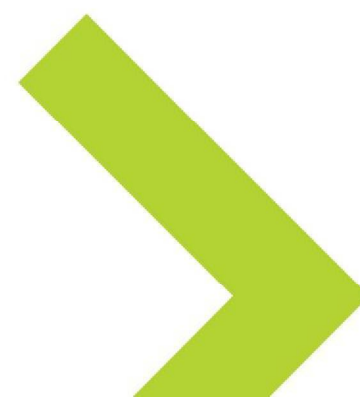
Vereniging Hogescholen [HV]. (2022). *Collectieve arbeids-overeenkomst voor het hoger beroepsonderwijs 2022-2023*.

Vereniging Hogescholen [VH]. (2024, 15 maart). Hogescholen maken bindende afspraken om instroom internationale studenten beperkt en in balans te houden [Persbericht].

Voets, B. (2022, 22 oktober). Dit HU-gebouw op het Utrecht Science Park kampt al dagen met een stroomstoring. *Algemeen Dagblad*.

Wassenaar, S., & Winters, B. (2023, 2 oktober). Pestgedrag, intimidatie en seksuele relaties tussen hoogleraren en studenten: op de Radboud Universiteit "overleef je alleen als je sterk bent". *De Gelderlander*.

Weerwind, F. M., & Van Huffelen, A. C. (2023, 30 mei). Antwoorden Kamervraag over het bericht 'Steekspel rond mysterieuze data-diefstal' Bedrijven delen data van klanten met hun leveranciers, maar hoe veilig is dat? [Kamerbrief].



COLOFON

Dit Risico- en Dreigingsbeeld is ontwikkeld door Clingendael in opdracht van het Platform Integrale Veiligheid Hoger Onderwijs (IV-HO).

Over Platform IV-HO

Het platform Integrale Veiligheid Hoger Onderwijs (IV-HO) is een samenwerkingsplatform, ondergebracht bij SURF, waar professionals van ho-instellingen kennis en ervaring uitwisselen t.b.v. een integraal veiligheidsbeleid. IV-HO is een initiatief van de Vereniging van Universiteiten (UNL) en de Vereniging Hogescholen (VH) en was tot december 2023 gesubsidieerd door het ministerie van Onderwijs Cultuur en Wetenschap (OCW).

Over Instituut Clingendael

Instituut Clingendael is een denktank en opleidingsinstituut op het gebied van internationale betrekkingen. Het instituut identificeert en analyseert politieke en sociale ontwikkelingen voor een breed scala aan nationale en internationale doelgroepen waaronder overheidsorganisaties, het bedrijfsleven en NGO's.

Auteurs van dit rapport

5.1.2e

© 2024



Op deze uitgave is de Creative Commons Naamsvermelding 4.0 licentie van toepassing. Maak bij gebruik van dit werk vermelding van de volgende referentie: Risico en Dreigingsbeeld (2024). Utrecht: Platform Integrale Veiligheid Hoger Onderwijs (IV-HO)

