

Dreigingsbeeld hoger onderwijs 2018





Colofon

Het dreigingsbeeld Hoger Onderwijs 2018 is in opdracht van het programma Integrale Veiligheid Hoger Onderwijs opgesteld door het COT Instituut voor Veiligheids- en Crisismanagement

Auteurs: Laurens van der Varst, Nico Kaptein, Frank Kuipers, Nils Dalmeijer

Rotterdam, juni 2018

Samenvatting dreigingsbeeld hoger onderwijs 2018

Achtergrond

Voor u ligt de 1ste editie van het dreigingsbeeld hoger onderwijs. Dit dreigingsbeeld is in opdracht van het programma Integraal Veilig Hoger Onderwijs (IV-HO) opgesteld door het COT Instituut voor Veiligheids- en Crisismanagement.

Het dreigingsbeeld is bedoeld als instrument. U kunt hiermee binnen de eigen hogeschool of universiteit, met het bestuur en medewerkers, de dialoog over veiligheid te voeren en afwegingen te maken. Hoe verhouden de uitkomsten van het dreigingsbeeld zich tot de dreigingen waarop u zich voorbereidt? Waar zitten nog kwetsbaarheden en wat betekent dat voor de bestaande aanpak van veiligheid?

Het dreigingsbeeld is gebaseerd op gesprekken met deskundigen op het gebied van onderwijs en/of veiligheid, publicaties, internetbronnen en een survey onder veiligheidscoördinatoren uit het hoger onderwijs. Centraal staan de acht thema's zoals gehanteerd binnen het programma IV-HO¹. Binnen deze thema's manifesteren zich specifieke dreigingen.

Het dreigingsbeeld geeft een actueel, landelijk beeld van dreigingen die spelen voor hogescholen en universiteiten. Die dreigingen zijn divers en kunnen per instelling verschillen. Elke hogeschool of universiteit heeft namelijk zijn eigen unieke kenmerken (activiteiten, ligging, organisatiestructuur, ambities). Die kenmerken beïnvloeden het veiligheidsrisicoprofiel.

Trends

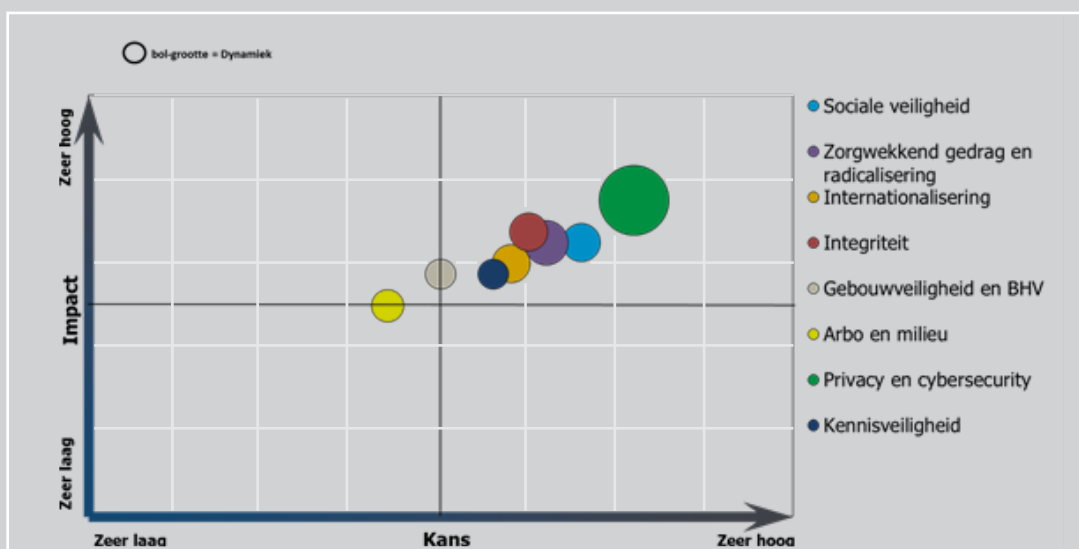
Wij signaleren enkele overkoepelende trends die invloed hebben op veiligheid en crisismanagement van hogescholen en universiteiten, namelijk:

1. Digitalisering
2. Internationale mobiliteit
3. Mondiale onveiligheid en onvoorspelbaarheid
4. Open campus, partnerschappen en 'shared workspaces'
5. Mediatisering: nieuwe media en 'fake news'
6. Afnemende risicotolerantie en aansprakelijkheid

Deze trends bieden kansen, maar ook bedreigingen. Het zijn krachten die inwerken op de veilige leer- en werkomgeving die hogescholen en universiteiten moeten bieden.

Dreigingen: een gevarieerd scala

Hogescholen en universiteiten worden geconfronteerd met een scala aan dreigingen. De onderstaande matrix laat zien welk thema hoog scoort: qua kans, qua impact en qua dynamiek. De acht thema's zijn ontleend aan het programma Integrale Veiligheid Hoger Onderwijs.



Figuur 3:
Dreigingsmatrix
van de thema's

¹ Het programma IV-HO hanteert in totaal tien thema's. Naast de genoemde thema's zijn dit Integrale veiligheid en Crisismanagement. Omdat uit deze thema's geen dreigingen voort komen, zijn ze hier buiten beschouwing gelaten.

Nieuwe dreigingen

Privacy en cybersecurity worden als belangrijkste dreiging gezien. De kans en potentiële impact van de dreiging worden als hoog tot zeer hoog beoordeeld. Als mogelijke verklaring geldt de nieuwe privacy verordening AVG (met sancties bij niet naleving), de omvang en hoge complexiteit van het vraagstuk en de mate waarin zich nieuwe ontwikkelingen voordoen. Als specifieke dreigingen komen uit onderzoek:

- Datalekken
- Manipulatie data en identiteitsfraude
- Spionage / verlies van intellectueel eigendom
- Reputatieverlies en aantasting van vertrouwen van studenten, medewerkers en andere belanghebbenden

Ook sociale veiligheid en zorgwekkend gedrag en radicalisering zijn dreigingen met een reële kans. Met name bij zorgwekkend gedrag en radicalisering signaleren respondenten de nodige dynamiek. Hier geldt, net als voor sociale veiligheid, dat de impact op de veiligheid van studenten en medewerkers groot is. Als specifieke dreigingen komen naar voren:

- Cyberpesten en –intimidatie
- Polariserend activisme dat gebruik maakt van nieuwe media
- Psychosociale en geestelijke gezondheidsproblemen/ suïcides

Bovenstaande zijn voorbeelden van nieuwe dreigingen. Dreigingen waarbinnen zich voortdurend nieuwe ontwikkelingen voordoen en waarvan de aanpak meerdere disciplines van organisaties raakt, zoals:

- Veiligheid en ICT Beveiliging
- Communicatie
- Juridische Zaken
- Bestuur
- Medewerkers en studenten

Dit zijn daardoor bij uitstek dreigingen waarvoor oplossingen in multidisciplinair verband gezocht moeten worden en deels in samenspraak met externe partners zoals de gemeente en politie. Bovendien zijn oplossingen niet altijd al uitgekristalliseerd. Hoe bijvoorbeeld de weerbaarheid tegen polariserend activisme of maatschappelijke spanningen versterken of omgaan met psychosociale gezondheidsproblemen van studenten? Hoe studenten en medewerkers daarin vanuit de organisatie ondersteuning en handelingsperspectief bieden? Dat vergt soms pionieren, open vizier houden voor wat er speelt binnen de school, met elkaar casuïstiek duiden en zoeken naar handelingsperspectief.

De impact van dreigingen blijft veelal niet beperkt tot één domein of discipline. Zo kan spionage bijvoorbeeld ‘raken’ aan cybersecurity, zorgwekkend gedrag en internationalisering. En is een datalek niet alleen een technisch ICT probleem, maar heeft een dergelijke incident al snel impact op meerdere terreinen, zoals onderzoek, communicatie, juridische zaken en bedrijfsvoering. De opgave is dan juist om vanuit een integrale benadering naar dergelijke ‘blended risks’, risico’s die (voorheen) afgebakende domeinen en disciplines overschrijden en doorkruisen, te kijken.

Kwetsbaar voor incidenten

De kans dat dreigingen zich manifesteren wordt door de bevroegde coördinatoren als hoog ingeschat. Dat sluit aan bij het beeld dat oprijst uit het incidentenoverzicht (bijlage) en gesprekken met respondenten. Daaruit blijkt dat zich, op de verschillende thema’s, met regelmaat incidenten voordoen bij hogescholen en universiteiten. Dan gaat het onder andere om grensoverschrijdend gedrag door studentenverenigingen, een aangifte wegens seksuele intimidatie tot een ontruiming van een onderwijsgebouw. Dat betekent niet dat de veiligheid en de veilige leer- en werkomgeving in het geding is. Wel zijn hogescholen en universiteiten kwetsbaar voor incidenten. Die incidenten kunnen, afhankelijk van omvang en ernst, grote impact uitoefenen op studenten en medewerkers en de continuïteit. Dit onder druk van maatschappelijke trends als polarisatie, mediatisering en afnemende risicotolerantie.

Klassieke dreigingen vergen aandacht en onderhoud

Opvallend is dat de kans en impact van meer klassieke dreigingen, zoals Arbo & milieu en gebouwveiligheid lager worden ingeschat, hoewel de potentiële impact op de veiligheid van studenten en medewerkers en de continuïteit van onderwijs hoog is. Als specifieke dreigingen worden genoemd: brand, chemicaliën ongevallen of ongevallen in laboratoria. Een mogelijke verklaring is dat dit gekende dreigingen zijn. Dreigingen waar een bestaand repertoire aan beheersmaatregelen tegenover gezet kan worden.

Dat maakt klassieke dreigingen niet minder belangrijk. De opgave ligt hier echter vooral in het goed uitvoeren en onderhouden van de beheersmaatregelen en BHV-procedures en alertheid op nieuwe situaties, zoals verandering in regelgeving, nieuwe eisen van Inspectie SZW en toezicht op brandveiligheidseisen in studentencomplexen op het campusterrein.

Weerbaar tegen dreigingen: vier reflectievragen voor de bestuurstafel

Dreigingen kunnen voor hogescholen en universiteiten grote impact hebben. Impact op de veiligheid van studenten en medewerkers, op de continuïteit en integriteit van onderwijs, op de reputatie. Bevorderen van de weerbaarheid tegen dreigingen is maatwerk, want elke instelling heeft zijn eigen bijzondere kenmerken (schaalgrootte, ambities, activiteiten). Om de stap van dit 'dreigingsbeeld 2018' naar de praktijk te faciliteren en het bestuurlijke gesprek over veiligheid binnen de hogescholen en universiteiten te bevorderen, formuleren we vier vragen die uitnodigen tot (bestuurlijke) reflectie.



1. Hoe verhoudt het dreigingsbeeld zich tot de dreigingen waarop onze hogeschool of universiteit zich voorbereid? Staan nieuwe dreigingen op onze bestuurlijke agenda?



2. Wat weten we over onze 'eigen' dreigingen? Welke sturingsinformatie hebben we?



3. Hoe bereiden wij ons voor op dreigingen: reactief, bewust accepteren van dreigingen, beleid maken, flexibel reageren? Wat is onze veiligheidsambitie?



4. Hoe is ons toezicht op veiligheid ingericht? Welke expertise kunnen we inschakelen om de weerbaarheid tegen specifieke dreigingen te bevorderen?

Inhoudsopgave

1	Inleiding	1
1.1	Achtergrond van het Dreigingsbeeld	1
1.2	Doel van het dreigingsbeeld	1
1.3	Dreigingen	1
1.4	Hoe is het dreigingsbeeld ontwikkeld?	2
1.5	Leeswijzer	3
2	Overkoepelende trends	4
2.1	Trends	4
3	Dreigingen per thema	7
3.1	Sociale veiligheid	7
3.2	Zorgwekkend gedrag en radicalisering	9
3.3	Internationalisering	10
3.4	Integriteit	12
3.5	Gebouwveiligheid	14
3.6	Arbo en milieu	16
3.7	Privacy en cybersecurity	17
3.8	Kennisveiligheid	19
4	Dreigingsbeeld	21
4.1	Integrale beoordeling dreigingen	21
4.2	Specifieke dreigingen	22
4.3	Impactgebieden dreigingen	23
5	Weerbaar tegen dreigingen: vier reflectievragen voor de bestuurstafel	24
6	Tot slot	26
	Bijlage 1 Beschrijving thema's	27
	Bijlage 2 Overzicht incidenten 2017 – 2018	28
	Bijlage 3 Coördinatoren groep en respondenten	30
	Bijlage 4 Achtergrondinformatie dreigingen	31
	Over het COT	32

1 Inleiding

1.1 Achtergrond van het Dreigingsbeeld

Het programma Integraal Veilig Hoger Onderwijs (IV-HO) heeft tot doel hogescholen en universiteiten te ondersteunen in het bieden van een veilige en integere werk- en leeromgeving voor studenten en medewerkers. In opdracht van het programma heeft het COT Instituut voor Veiligheids- en Crisismanagement een dreigingsbeeld hoger onderwijs ontwikkeld.

Voor u ligt de eerste editie van het dreigingsbeeld. Voor de eerste keer is zo'n breed scala aan dreigingen voor hogescholen en universiteiten in samenhang in beeld gebracht. Het spreekt voor zich dat de dreigingen uit dit dreigingsbeeld 'vertaald' moeten worden naar de eigen hogeschool of universiteit. Daarvoor biedt dit dreigingsbeeld bruikbaar aanknopingspunten.

We zijn ervan overtuigd dat met dit dreigingsbeeld de dialoog over dreigingen – en de interne governance rond integrale veiligheid - binnen de scholen naar een volgend niveau getild kan worden. Naast inzichten wensen wij u ook een succesvolle toepassing van het dreigingsbeeld in uw eigen onderwijsomgeving toe.

1.2 Doel van het dreigingsbeeld

Het dreigingsbeeld is een instrument om binnen de eigen hogeschool of universiteit, met het bestuur en medewerkers de dialoog over veiligheid te voeren. Hoe verhouden de uitkomsten van het dreigingsbeeld zich tot de dreigingen binnen onze instelling? Hoe is onze organisatie voorbereid op de geïdentificeerde dreigingen? Waar zitten nog kwetsbaarheden en wat betekent dat voor onze aanpak? Welke risico's accepteren we, welke niet en welke prioriteiten stellen we? En hoe sturen we op veiligheid?

Het dreigingsbeeld geeft een actueel, landelijk beeld van dreigingen die spelen voor hogescholen en universiteiten. Die dreigingen zijn divers en kunnen per instelling verschillen. Elke hogeschool of universiteit heeft namelijk zijn eigen unieke kenmerken (activiteiten, ligging, organisatiestructuur, ambities). Die kenmerken beïnvloeden het veiligheidsrisicoprofiel. Niettemin zijn er ook dreigingen die voor alle hogescholen en universiteiten spelen; die staan in dit dreigingsbeeld.

1.3 Dreigingen

In dit dreigingsbeeld staan de acht thema's zoals gehanteerd binnen het programma IV-HO centraal (zie afbeelding, bijlage 1 voor definitie)². Binnen deze thema's manifesteren zich specifieke dreigingen. Een voorbeeld ter verduidelijking: binnen het thema Privacy en cybersecurity spelen meerdere dreigingen, zoals datalekken of -manipulatie. Ook kan een bepaalde dreiging onder meerdere thema's vallen. Zo kan spionage bijvoorbeeld 'raken' aan cybersecurity en internationalisering. En is een datalek niet alleen een technisch ICT probleem, maar heeft een dergelijke incident al snel impact op meerdere terreinen, zoals onderzoek, communicatie, juridische zaken en bedrijfsvoering. De opgave bij dergelijke 'blended risks', risico's die domeinen en disciplines overschrijden en doorkruisen, is juist vanuit een integrale blik te kijken naar mogelijke beheersmaatregelen.



² Het programma IV-HO hanteert in totaal tien thema's. Twee van de tien thema's zijn niet opgenomen als thema's van dit dreigingsbeeld: thema's Integrale veiligheid en Crisismanagement.

Wat is een dreiging?

Onder een dreiging verstaan we in het kader van dit dreigingsbeeld: “een gebeurtenis waarbij de veiligheid van studenten en/of medewerkers, de continuïteit/ integriteit van onderwijs en/of onderzoek en de reputatie van de organisatie in het geding zijn”.

Die dreiging kan moedwillig zijn of per toeval ontstaan of bewust of onbewust bestaan en zowel ‘van buiten’ als ‘van binnen’ komen. Een dreiging kan voor hogescholen en universiteiten op meerdere terreinen impact hebben. In dit dreigingsdreigingsbeeld staan drie impactgebieden centraal:

1. veiligheid van studenten en/of medewerkers
2. onderwijs en/of onderzoek
3. reputatie en bedrijfsvoering

1.4 Hoe is het dreigingsbeeld ontwikkeld?

Dit dreigingsbeeld is gebaseerd op interne en externe bronnen. Bijvoorbeeld gesprekken met deskundigen op het gebied van onderwijs en/of veiligheid, publicaties, internetbronnen en een survey onder (integrale) veiligheidscoördinatoren uit het hoger onderwijs.

Welke bronnen raadplegen veiligheidscoördinatoren?

Interne bronnen

- Incidentenregistraties
- Interne jaarverslagen
- Risico analyses
- RI&E

Externe bronnen

- Politie/ GGZ/ VNG & Gemeenten
- Centrum Informatiebeveiliging en Privacybescherming
- Contacten met collega instellingen
- SURF Community voor Informatiebeveiliging en Privacy
- SURFnet Community van Incident Response Teams
- URF Cyberdreigingsbeeld
- Security websites
- NCTV/NCSC/AIVD
- IV-HO veiligheidsfiches
- Vaktijdschriften
- Wetenschappelijke publicaties (Ulrich Beck: Risk Society)
- Recent onderzoek (Crisislab)
- Kenniscentrum Evenementenveiligheid

Op basis van informatie is een lijst met relevante trends en specifieke dreigingen opgesteld. Vervolgens is een online survey uitgevoerd onder de coördinatoren. In de survey zijn respondenten gevraagd specifieke dreigingen, de thema's en de overkoepelende trends te beoordelen. De survey is in april en mei 2018. In totaal 36 (integrale) veiligheidscoördinatoren hebben deelgenomen aan de survey. De opbrengsten zijn besproken met de coördinatoren groep.

Een bedreiging is niet statisch; bedreigingen ‘komen en gaan’, zoals de Raad van Advies van IV-HO in zijn advies over veiligheid in het onderwijs opmerkt.³ Dat houdt in dat ze gekleurd worden, conjunctuurgevoelig, afhankelijk van perceptie en aan verandering onderhevig zijn.⁴ Ter illustratie: algemeen bekend is bijvoorbeeld dat terrorisme door burgers als een zeer grote dreiging wordt gezien, hoewel de kans daadwerkelijk slachtoffer te worden van een aanslag uitermate klein is.⁵ Dergelijke

nieuwe dreigingen als terrorisme en cyber worden in het algemeen als riskanter gepercipieerd, dan meer alledaagse, ‘vertrouwde’ dreigingen⁵.

In het licht van percepties van dreigingen maken wij twee kanttekeningen: 1) voor het beoordelen van de dreigingen heeft een uitvraag plaatsgevonden onder een specifieke doelgroep, namelijk adviseurs Integrale Veiligheid. Verwacht wordt dat zij, gelet op hun werkzaamheden op het gebied van de verschillende aspecten van (integrale) veiligheid, in staat zijn tot een gefundeerde inschatting van dreigingen. Maar hun beoordeling kan en zal ook gekleurd zijn, omdat zij vanuit hun professie dagelijks met dreigingen te maken hebben. Hun inschatting van dreigingen zal anders zijn dan dat van docenten, baliepersoneel of studenten. 2) de beoordeling van de dreigingen vond ruim een maand voor het ingaan van de nieuwe Europese privacy verordening (AVG) plaats. Mogelijk heeft de timing van de survey effect gehad op de uitkomsten, bijvoorbeeld doordat de respondenten dreigingen binnen het thema Privacy en cybersecurity hoger inschatten. Waar dergelijke kleuringen door de actualiteit worden verondersteld, is dit in het dreigingsbeeld aangegeven.

1.5 Leeswijzer

Hoofdstuk 2 bevat overkoepelende trends die invloed hebben op veiligheid en crisismanagement van hogescholen en universiteiten. Hoofdstuk 3 bevat de ontwikkelingen en dreigingen voor acht thema's van Integrale Veiligheid Hoger Onderwijs. In hoofdstuk 4 staat de duiding van dreigingen centraal. Hoofdstuk 5 sluit af met vier reflectievragen voor de interne dialoog over weerbaarheid tegen dreigingen.

In bijlage 1 staan de acht thema's toegelicht. In bijlage 2 is een overzicht met incidenten in de periode 2017-2018 opgenomen. Bijlage 3 bevat de coördinatoren groep en respondenten, bijlage 4 de geraadpleegde bronnen.



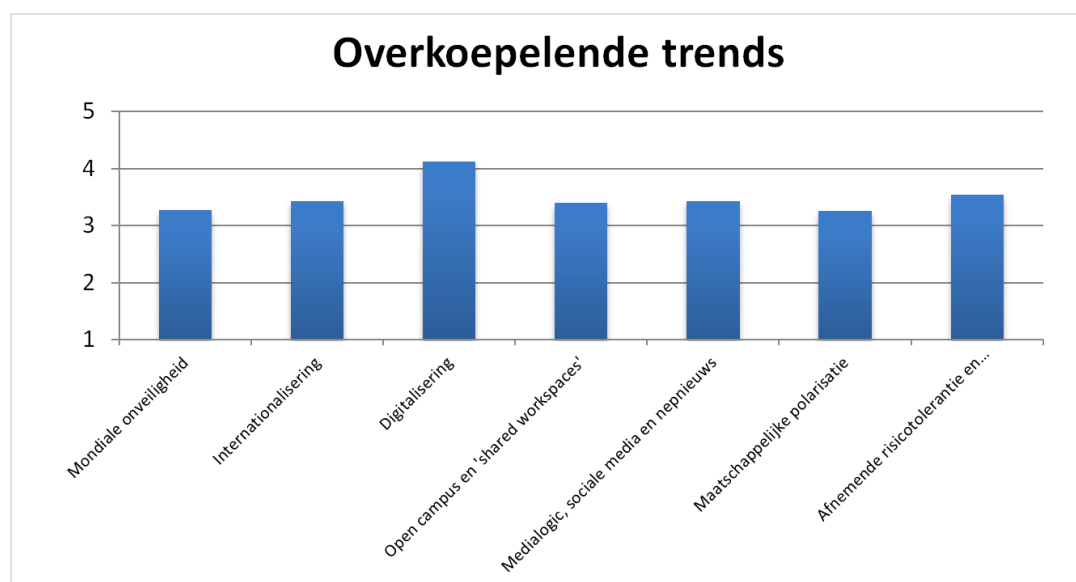
5 https://www.nctv.nl/onderwerpen_a_z/Risico-en-crisisbarometer/index.aspx

6 Slovic, *The perception of risk*, 2016.

2 Overkoepelende trends

In dit hoofdstuk staan enkele overkoepelende trends die invloed hebben op veiligheid en crisismangement van hogescholen en universiteiten centraal. De lijst is opgesteld na bestudering van publicaties en overleg met de coördinatoren. Vervolgens zijn de trends ter beoordeling uitgevraagd in de survey.

2.1 Trends



Figuur 2: Impact van overkoepelende trends op het hoger onderwijs

- 1. Groeiende mondiale onveiligheid en onvoorspelbaarheid:** De algemene indruk is dat de mondiale veiligheidssituatie is verslechterd. Er is sprake van meer onveiligheid en grotere onvoorspelbaarheid. Dat is zichtbaar in onder meer terroristische aanslagen in Parijs, Brussel en Londen en snelle veranderingen in de politieke situatie in landen als Turkije. Ook de dreiging van terrorisme is nog steeds hoog.⁷ Volgens deskundigen heeft de terugkeer van geopolitiek nog niet daadwerkelijk geresulteerd in meer conflicten en grotere onzekerheid, maar is er zeker reden voor zorg.⁸
- 2. Internationale mobiliteit:** De verwachting is dat de internationale mobiliteit van studenten en medewerkers, het grensoverschrijdend werken, studeren en opdoen van (stage) ervaringen de komende jaren aanhoudt. Uit recente gegevens van Nuffic blijkt dat de internationale studentenpopulatie in Nederland steeds meer divers wordt. Internationale studenten maken gemiddeld 12,2% uit van de gehele studentenpopulatie. Bijna 90.000 daarvan volgen een volledige studie, de rest komt voor een korter verblijf zoals een uitwisseling via het mobiliteitsprogramma Erasmus+. Tegelijkertijd presenteerde minister van Onderwijs Ingrid van Engelshoven in mei 2018 een akkoord om samen met de vereniging van universiteiten VSNU en de Vereniging Hogescholen het aantal internationale studenten terug te dringen.⁹

Circa 1 op de 4 internationale studenten komt van buiten de Europese Economische Ruimte (EER). De Duitse studenten zijn goed voor bijna 25% van de totale internationale studentenpopulatie. China staat met 4.475 studenten op de tweede plek. De aantallen Duitse en Chinese studenten nemen echter iets af terwijl het aantal studenten met een andere nationaliteit toeneemt. Daardoor wordt de internationale studentenpopulatie jaar na jaar steeds gevarieerder.¹⁰

⁷ https://www.nctv.nl/binaries/DTN46%20Samenvatting_tcm31-289786.pdf

⁸ <https://www.clingendael.org/pub/2017/monitor2017/multiorder/>

⁹ <https://www.nrc.nl/nieuws/2018/05/10/student-uit-buitenland-afremmen-a1602588>

¹⁰ <https://www.nuffic.nl/nieuws/nuffic-news/internationale-studentenpopulatie-steeds-diverser>

3. **Digitalisering:** Digitalisering neemt toe in alle facetten van het dagelijks leven van studenten en medewerkers. Dat leidt tot meer aandacht voor ICT in opleidingen, toename van ICT gebruik voor onderwijs en onderzoek en tot het permanent met elkaar in verbinding staan van burgers via moderne communicatiemiddelen. Het delen van informatie en kennis groeit en wordt eenvoudiger met maximale transparantie als resultaat.¹¹

Het Internet of Things (IoT) is de ontwikkeling waarin steeds meer apparaten en mobiele devices via het internet aan elkaar zijn verbonden. De ontwikkeling van het Internet of Things biedt allerlei kansen, maar is de afgelopen jaren ook kwetsbaar gebleken.¹² Onveilige apparaten kunnen zijn of worden besmet en misbruikt voor bijvoorbeeld DDOS aanvallen. Ook hogescholen en universiteiten kunnen hiermee geconfronteerd worden. Hierbij kan gedacht worden aan gebouwbeheerssystemen en sensoren in laboratoria. De groei van het aantal IoT-apparaten en de kwetsbaarheid ervan, leidt tot een grotere dreiging.¹³ Daarnaast waarschuwt SURF dat studenten, docenten, onderzoekers en andere medewerkers vaker gebruik maken van mobiele apparaten, zoals smart phones of tablets. Digitalisering en globalisering dragen er ook toe bij dat grenzen tussen externe en interne veiligheid verder vervagen.¹⁴ Conflicten die elders plaatsvinden kunnen daardoor ook in Nederland effect hebben.

4. **Medialogica, sociale media en fake news:** Het gebruik van smartphone en ipad, waarmee studenten permanent online en bereikbaar zijn en het gebruik van Facebook, Twitter en Whatsapp is alomtegenwoordig. Dat betekent dat informatie razendsnel kan worden gedeeld en verspreid en dat de beschikbaarheid van informatie toeneemt.

Recent is er veel aandacht voor nepnieuws ('fake news'). Daaronder wordt misleidende informatie verstaan die wordt verspreid uit financieel gewin of voor het beïnvloeden van de publieke opinie. Grenzen tussen feitelijke informatie en nepnieuws vervagen, waardoor het onderscheid tussen 'echt, betrouwbaar, feitelijk' en 'nep, subjectief, mening' lastiger is te onderscheiden.¹⁵ Dat vormt een gevaar voor gefundeerde oordeelsvorming, kan tot escalatie van incidenten leiden en het vertrouwen in (wetenschappelijke) instanties, zoals hogescholen en universiteiten en in wetenschap aantasten.

Gevaar is dat er een bepaald beeld van een persoon of gebeurtenis kan worden neergezet, waarin die beeldvorming zijn eigen dynamiek en leven gaat leiden. Die medialogica, waarin het beeld van de persoon of gebeurtenis een nieuwe realiteit wordt, is een situatie waarmee bestuurders en docenten kunnen worden geconfronteerd. Het zaaien van twijfel is soms al voldoende om een instelling of persoon in diskrediet te brengen.

5. **Open campus, partnerschappen en 'shared workspaces'** Eén van de ontwikkelingen is die van de open campus; regionale scienceparken waar universiteiten, hogescholen, onderzoeksinstituten en bedrijven zijn gevestigd. Binnen die scienceparken is een grote diversiteit aan functies (onderwijs, ontmoeting, onderzoek, wonen, werk, sport), werknemers en organisaties actief.

De campus heeft daarmee een veranderde functie gekregen, waarin naast het voorzien in een veilige en gezonde werkplek het bieden van een inspirerende ontmoetingsplaats voor gebruikers ('campus community') aan belang toeneemt. Tevens groeide het aantal andere partijen dat op de campus actief is, zoals onderzoeksinstituten, start-ups en andere bedrijven.¹⁶

Die diversiteit zorgt voor de nodige complexiteit en beheers- en verantwoordelijkheidsvraagstukken. Hoe ver reikt de verantwoordelijkheid voor veiligheid van een hogeschool of universiteit? Welke veiligheidseisen stellen we aan gedeelde werkomgevingen? Welke normen hanteren we als hogeschool (en hoe verhouden die normen zich tot eisen van andere partijen op de campus)?

6. **Maatschappelijke polarisatie:** Er lijkt in Nederland sprake van groeiende maatschappelijke polarisatie: ervaren tegenstellingen tussen groepen worden groter, standpunten extremer. De ruimte

11 <http://www.vsnul.nl/files/documents/Campus%20NL%20digital%20version%20%28for%20websites%29.pdf>

12 CSBN 2017.

13 SURF, Cyber dreigingsbeeld 2017.

14 AIVD, Jaarverslag 2017, 2018.

15 <https://www.mediawijsheid.nl/nepnieuws/>

16 <http://www.vsnul.nl/files/documents/Campus%20NL%20digital%20version%20%28for%20websites%29.pdf>

voor dialoog en inleving in anderzans' positie neemt af. Die polarisatie en identiteitspolitiek dringt ook tot het onderwijs, zo waarschuwt o.a. de voorzitter van het College van Bestuur van Hogeschool Rotterdam¹⁷ en de voorzitter CvB van de Universiteit Leiden.¹⁸

- 7. Afnemende risicotolerantie en verantwoording.** Nederland is relatief gezien een veilig land: de criminaliteit daalt al jaren, de kans op slachtofferschap neemt af.¹⁹ Niettemin is sprake van afnemende risicotolerantie en verantwoordingsdruk als zich inbreuken op veiligheid voordoen. Waar incidenten vroeger werden afgedaan als 'wil van God' of louter pech, staat nu aansprakelijkheid centraal.²⁰ Wie is verantwoordelijk voor het 'falen'? Wat heeft diegene gedaan of juist nagelaten om deze inbreuk te voorkomen?

17 <https://www.nrc.nl/nieuws/2018/04/03/naast-de-ikstaat-een-wij-wanneer-zien-politici-dat-a1597915>

18 <https://www.volkskrant.nl/columns-opinie/waarom-ik-hoogleraren-niet-tot-de-orde-roep-b439903e/>

19 CBS, *Het mysterie van de verdwenen criminaliteit*, 2018.

20 <http://crisislab.nl/wordpress/wp-content/uploads/Risk-analysis-HEIs.pdf>



3 Dreigingen per thema

Dit hoofdstuk beschrijft specifieke dreigingen binnen de acht IV-HO thema's. Verder zijn per thema de resultaten van de survey opgenomen: de beoordeling van de acht thema's op kans, impact en dynamiek. Ter illustratie zijn nieuwsitems van incidenten opgenomen.

3.1 Sociale veiligheid

Sociale veiligheid is een ruim begrip. Een scala aan gedrag kan de sociale veiligheid van medewerkers en studenten aantasten, zoals discriminatie, diefstal, intimidatie, agressie en geweld. Voor het hoger onderwijs worden, in tegenstelling tot bijvoorbeeld het middelbaar onderwijs, niet structureel gegevens verzameld over het aantal incidenten.²¹ Daardoor ontbreekt een landelijk beeld van de omvang van dit vraagstuk.

(Online) bedreigingen. Dreigingen aan het adres van Hoger Onderwijs instellingen komen met regelmaat voor, via een dreigtelefoontje of online. Een voorbeeld zijn de recente valse bedreigingen bij internationale scholen in Maastricht, Den Haag en Utrecht in oktober 2017.²² Dergelijke dreigingen zorgen voor bestuurlijke dilemma's, omdat het lastig kan zijn de dreiging te beoordelen en hierop passend te reageren. Gelijktijdig kunnen gerichte dreigingen aan het adres van individuele medewerkers de nodige persoonlijke impact hebben op de betreffende persoon en zijn of haar naasten.

Daling criminaliteit. Landelijk is een trend zichtbaar van afnemende (geregistreerde) criminaliteit, zoals diefstal, vandalisme en geweld en een stijging van het veiligheidsgevoel.²³ De recente International Fear of Crime Trend Index toont eveneens een gestage verbetering van de beleving van veiligheid in Nederland (zie grafiek). Hierin zijn overigens de meer klassieke dreigingen opgenomen, zoals overlast en criminaliteit en minder meer actuele zoals terrorisme en cybercrime.²⁴

Maatschappelijke polarisatie. Er lijkt sprake in Nederland van groeiende maatschappelijke polarisatie: ervaren tegenstellingen tussen groepen worden groter, standpunten extremer. De ruimte voor dialoog en inleving in andermans' positie neemt af. Die polarisatie en identiteitspolitiek dringt ook tot het onderwijs, zo waarschuwt de voorzitter van het College van Bestuur van Hogeschool Rotterdam.²⁵ Polarisation kan zich op meerdere manieren in het onderwijs manifesteren, bijvoorbeeld tijdens colleges (wanneer studenten het debat opzoeken met docenten of collega-studenten over maatschappelijk beladen thema's als de repercussies als gevolg van de coupoging in Turkije) of op het schoolplein. Een andere manifestatievorm, waarvoor de Raad van Advies aandacht vraagt, is de vrije meningsvorming die binnen hogescholen en universiteiten onder druk staat van polariserend activisme; activisme dat daarbij gebruik maakt van sociale media en klachtprocedures. Zij signaleren een tendens waarin wetenschappers en docenten het debat in de klas en met de samenleving schuwen en kiezen voor zelfcensuur uit zelfbescherming.²⁶

Toename psychische klachten. Studenten in het hoger onderwijs hebben te maken met psychische klachten. Belangrijke oorzaak hiervoor is, naast reeds eerder ontstane problemen in de privésfeer, ervaren prestatiedruk. Deze druk komt niet alleen vanuit het onderwijs en regelgeving, maar ook van bijvoorbeeld sociale media die een grote bijdrage leveren aan het zelfbeeld van jongeren en de daarmee samenhangende 'Fear of Missing Out'. Dit leidt tot een toename van stress, angststoornissen, burn-outklachten, en een toename onder studenten van concentratie-bevorderende middelen als amfetaminen en Ritalin (ook zonder AD(H)D). Ook gebruiken studenten met problemen bovengemiddeld veel alcohol.²⁷

Cyberpesten. Uit cijfers van het CBS blijkt dat in 2014 ruim 400 duizend mensen van 15 jaar en ouder wel eens gepest te zijn op internet. Ruim 11 procent van de jongeren tussen de 15 en 18 jaar werd geconfronteerd met cyberpesten, tegenover ruim 5 procent van de 21- tot 25-jarigen. Naarmate de

21 <https://www.schoolenveiligheid.nl/actueel/herinnering-jaarlijkse-monitoring-sociale-veiligheid/>

22 <https://www.rtlnieuws.nl/nederland/golf-van-valse-bommeldingen-op-scholen-door-heel-nederland>

23 <https://www.cbs.nl/nl-nl/nieuws/2018/09/afname-criminaliteit-in-alle-delen-nederland>

24 <https://ccv-secondant.nl/platform/article/veiligheidsbeleving-in-nederland-toont-positief-beeld/>

25 <https://www.nrc.nl/nieuws/2018/04/03/naast-de-ikstaat-een-wij-wanneer-zien-politici-dat-a1597915>

26 Raad van Advies, Advies over veiligheid in het hoger onderwijs.

27 <https://www.windesheim.nl/over-windesheim/nieuws/2018/april/actieplan-studentenwelzijn-pleit-voor-integrale-aanpak/>

leeftijd vordert krijgen Nederlanders minder met cyberpesten te maken. Meest voorkomende vormen van cyberpesten zijn laster, stalken en bedreiging met geweld. Laster is het verspreiden van foto's, kwetsende teksten of roddel via het internet. Chantage als vorm van cyberpesten komt minder voor.²⁸

Sexting. Sexting is het online uitwisselen van naaktfoto's of seksfilmpjes. Uit onderzoek van Rutgers blijkt dat 1 op de 8 jongeren in het eerste halfjaar van 2017 een naaktfoto of seksfilmpje van zichzelf naar iemand heeft verstuurd. Sexting wordt meestal vrijwillig en met toestemming gedaan, het heeft dan de betekenis van flirten. Over het algemeen weten jongeren zich goed te beschermen tegen online risico's. In sommige gevallen is geen sprake van toestemming, maar worden beelden toch gedeeld. De consequenties (schaamte, reputatieverlies) voor slachtoffers kunnen groot zijn.²⁹

Suicide. Zelfmoord is de nummer twee doodsoorzaak onder studenten volgens het Bureau Studentenzaken in Amsterdam. Uit onderzoek van dit bureau blijkt dat één procent van de tienduizend deelnemers wel eens een zelfmoordpoging heeft gedaan. Naar schatting heeft drie procent van de studenten wel eens aan zelfmoord gedacht. De hoge prestatiedruk, een onbekende omgeving, een onregelmatig slaapritme en het drank- en drugsgebruik maken studenten tot een kwetsbare groep. Begin 2017 is er een protocol ter preventie van zelfmoord opgesteld door de studentenartsen aan de UvA³⁰.

Nieuwsitem

Universiteit Leiden bedreigd

In de avond van maandag 5 oktober 2015 verschijnt er een anonieme bedreiging aan het adres van de Universiteit Leiden op het internetforum 4chan. *'Tomorrow at 10.05 I will open fire at the university of Leiden. Not gonna tell you which faculty, that up to you to guess.'* De universiteit besloot niet te ontruimen maar meerdere locaties, ook in Den Haag, werden bewaakt door de politie. Rond het middag uur, toen het genoemde tijdstip al lang verstreken was, werd de bewaking opgeheven. De volgende nacht heeft de politie een 21-jarige verdacht aangehouden voor de bedreiging.³¹

Geweldsincident

Bij een geweldsincident in Wageningen zijn twee gewonden gevallen. Dat meldt de politie Gelderland op Twitter. Het incident vond plaats op de campus van de universiteit Wageningen. De exacte toedracht is onbekend. De verdachte kon al snel worden aangehouden. In een sloot werd hij door agenten aangetroffen. Volgens de politie maakte de man een verwarde indruk. Over zijn identiteit kon een woordvoerder van de politie Gelderland nog niets zeggen.³²

Beoordeling van kans, impact en dynamiek. Het hoofdthema "Sociale veiligheid" scoort hoog op alle drie de bevestigde variabelen. Vooral de kans dat een dreiging die binnen het thema van "Sociale veiligheid" valt zich voordoet is sterk aanwezig binnen het beeld van (integrale) veiligheidscoördinatoren. Meer dan de helft van de coördinatoren beoordeelde de kans als hoog.

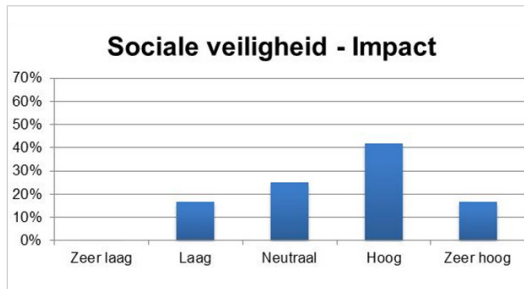
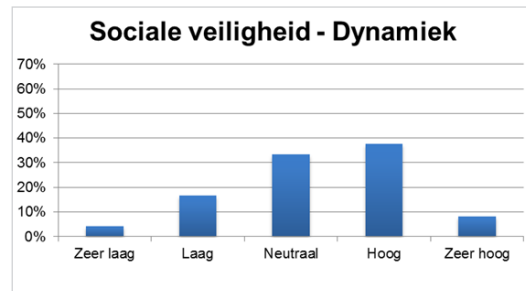
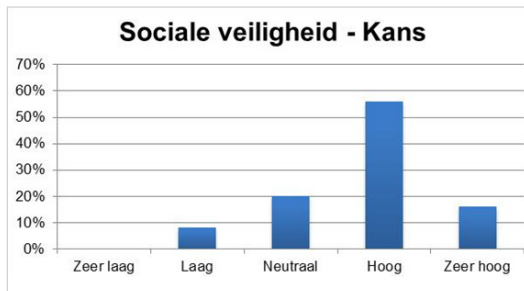
28 <https://www.cbs.nl/nl-nl/nieuws/2015/34/bijna-8-procent-van-de-jongeren-gepest-op-het-internet>

29 <http://seksonderje25e.nl/files/uploads/Onderzoeksboek%20Seks%20onder%20je%2025e%202017.pdf>

30 https://www.huisartsenamsterdam.nl/wp-content/uploads/2016/12/Richtlijnen-signalering-en-vervolgstappen-suiciderisico.pdf?_sp=27c0835d-f0c6-4613-98f0-b3ae18e4bc0b.1521797887830

31 <https://www.nrc.nl/nieuws/2015/10/06/extra-politiebewaking-na-dreigement-aan-universiteit-leiden-a1412599>

32 <https://www.nrc.nl/nieuws/2018/01/18/twee-gewonden-bij-geweldsincident-universiteit-wageningen-a1588800>



Figuren 5, 6 en 7:
Beoordeling kans, impact en dynamiek van Sociale veiligheid

3.2 Zorgwekkend gedrag en radicalisering

Zorgwekkend gedrag is gedrag of signalen die wijzen op de bereidheid geweld te gebruiken of hiermee te dreigen. Die bereidheid kan voortkomen uit bijvoorbeeld ideologische overtuigingen of geestelijke problematiek. Voorbeelden van dreigingen zijn huiselijk geweld, radicalisering, bedreigingen, agressie en geweld.

Veel aandacht en hulpmiddelen; feitelijke gegevens over dreigingen beperkt. Er zijn meerdere handreikingen en (online) trainingsmodules beschikbaar voor het herkennen en omgang met zorgwekkend gedrag.³³ Hoewel er veel hulpmateriaal beschikbaar is, valt op dat openbaar toegankelijke informatie over omvang, aard en ernst van casussen in het hoger onderwijs ontbreekt. Dat kan te maken hebben met vertrouwelijkheid of terughoudendheid om dergelijke informatie te delen. Een uitzondering is Hogeschool Rotterdam. Zij melden in het jaarverslag 48 geanonimiseerde incidenten rond zorgwekkend gedrag in het afgelopen studiejaar. Daarbij ging het om tien incidenten (eenmalige gebeurtenissen van signalen met beperkte afmetingen), tien terugkerende incidenten (herhaalde gebeurtenis met een duidelijke uitstraling naar de omgeving) en 17 casus zorgwekkend gedrag (reële dreiging voor studenten, medewerkers of derden).³⁴ Zorgwekkend gedrag en radicalisering wordt door respondenten wel als een kansrijke en dynamische dreiging gezien.

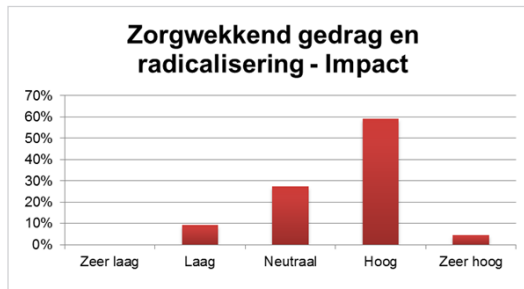
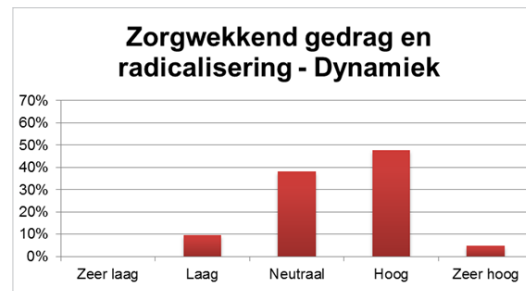
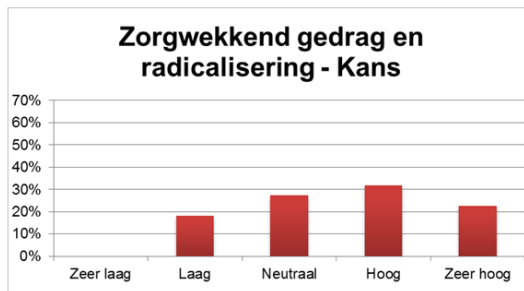
Radicalisering en polarisatie: De NCTV vraagt aandacht voor personen die nooit zijn uitgereisd, maar geïnspireerd en aangestuurd worden door jihadistische organisaties. Jihadisten zouden zich meer richten op missiewerk (da'wa) en het actief uitdragen van het gedachtegoed. Daarbij leidt het maatschappelijke debat over salafisme en de gespannen verhoudingen in Turkije volgens de NCTV tot gepolariseerde stellingnames.³⁵

Beoordeling van kans, impact en dynamiek. De (integrale) veiligheidscoördinatoren zijn verdeeld over de kans dat er dreigingen zich voordoen binnen het thema Zorgwekkend gedrag en radicalisering, aangetoond door de redelijk gelijke verdeling van de kans beoordeeld als laag tot de kans beoordeeld als zeer hoog. Het beeld van de impact en de dynamiek van dreigingen binnen het thema Zorgwekkend gedrag en radicalisering is minder verdeeld. Een groot deel van de (integrale) veiligheidscoördinatoren beoordeelt zowel de impact als de dynamiek als hoog.

³³ Zie bijvoorbeeld de e-learning zorgwekkend gedrag en handreiking signalering en begeleiding veiligheid- en leefstijlrisico's.

³⁴ Hogeschool Rotterdam, Jaarverslag Integrale Veiligheid 2016-2017.

³⁵ https://www.nctv.nl/binaries/DTN47%2C%20infographic_tcm31-310572.pdf



Figuren 8,9 en 10:
Beoordeling kans, impact en dynamiek van Zorgwekkend gedrag en radicalisering

3.3 Internationalisering

Bij internationalisering gaat het om dreigingen die verbonden zijn aan internationale mobiliteit van studenten en medewerkers van hogescholen en universiteiten, in het kader van uitwisselingsprogramma's, stages en onderzoeken. Hierbij gaat het zowel om uitgaande als inkomende mobiliteit.

Geopolitieke spanningen en mondiale conflicten. De algehele indruk is dat van een toename van de mondiale onveiligheid, resulterend in meer risicolanden en negatieve reisadviezen. Dat wordt bevestigd door de jaarlijkse terrorisme en politiek geweld monitor. Daaruit wordt zichtbaar dat de risico's op politiek geweld wereldwijd stijgen als gevolg van groeiende geopolitieke spanningen, de afbrokkeling van liberaal-democratische regeringen en de gevolgen van wereldwijde conflicten. De politieke risico's zijn in 2017 in elf landen gestegen. In slechts twee landen namen ze af. Meer specifiek stond in 2017:

- 40 procent van alle landen bloot aan risico's op terrorisme en sabotage;
- had 60 procent te maken met risico's op civiele onrust
- 33 procent met risico's op opstanden, oorlog of coups.
-

In totaal werden 163 landen in 2017 beoordeeld op hun gevoeligheid voor maatschappelijke onrust, terrorisme, sabotage, opstanden, oorlog of coups. Per saldo werd de situatie wereldwijd minder veilig. De risicoscores namen toe in Bosnië & Herzegovina, Ethiopië, Finland, Honduras, Macedonië, Myanmar, Noord-Korea, Noorwegen, Polen, Slowakije, Spanje, Togo, Trinidad & Tobago, Tsjechië, Venezuela, Wit-Rusland en Zuid-Korea. In Angola, Gambia, Kenia, Madagaskar, Portugal en Zimbabwe namen de risico's juist af.³⁶

De afgelopen jaren deden zich meerdere aanslagen voor. Uit een onderzoek van DUO Onderwijsonderzoek & Advies onder 217 directeuren in het voortgezet onderwijs leidde dit onder een kwart van de scholen tot een wijziging van de bestemming. Hoewel Londen, Parijs en Berlijn het vaakst werden geschrapt, blijven het nog steeds de populairste bestemmingen.³⁷ Ook veranderde politieke verhoudingen in uitwisselingslanden kan leiden tot risico's of juist toenemende onzekerheid. Uit navraag van de NOS blijkt dat sommige hogescholen een afname van studenten zien die voor uitwisseling of studie naar Turkije afreizen.³⁸ Verder zijn met enige regelmaat studenten slachtoffer van ongevallen of natuurrampen tijdens hun verblijf in het buitenland.

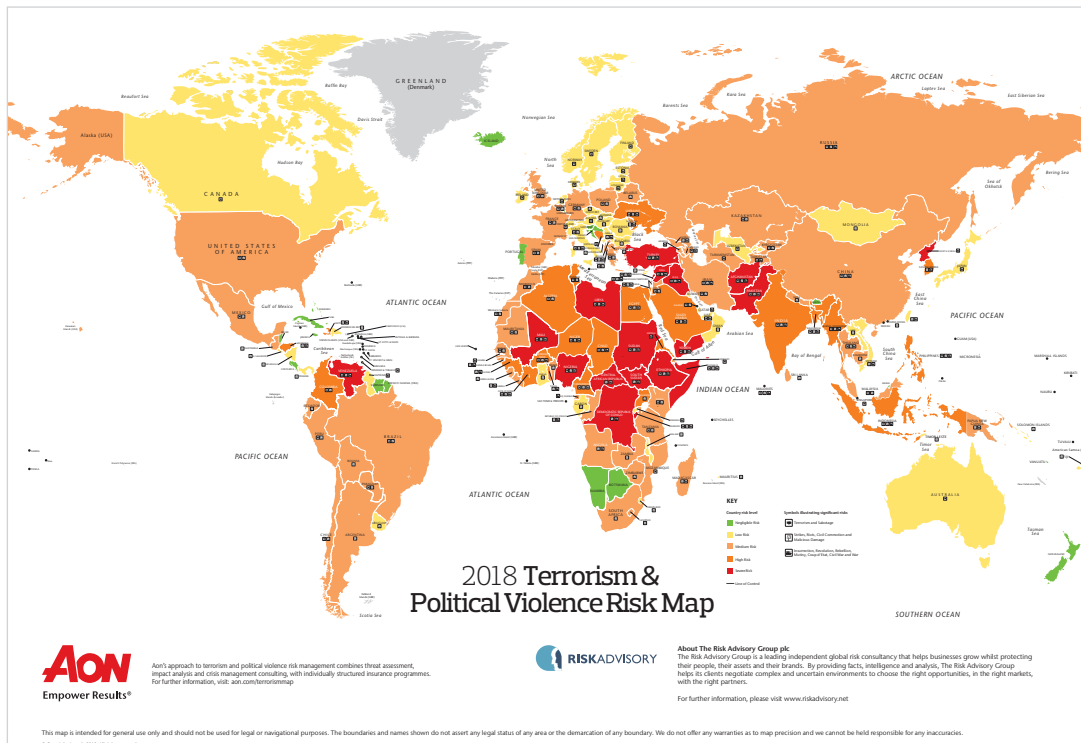
Meer internationale studenten. Het aantal studenten dat vanuit het buitenland in Nederland komt studeren, groeit, zowel voor voltijd hbo-master als voltijd wo-bachelor en -master. De internationale instroom bestaat voor het grootste deel uit studenten uit de Europese Unie.³⁹

³⁶ <http://www.managersonline.nl/nieuws/19544/bedrijfsleven-onder-druk-door-politieke-risicos-en-politiek-geweld.html>

³⁷ <http://www.duo-onderwijsonderzoek.nl/wp-content/uploads/2018/02/Rapportage-Buitenlandse-reizen-in-het-VO-13-februari-2018.pdf>

³⁸ <https://nos.nl/op3/artikel/2153630-veel-minder-studenten-gaan-naar-turkije.html>

³⁹ Inspectie OCW, *De staat van het onderwijs 2016-2017*.



Veiligheid als randvoorwaarde voor internationalisering. Binnen hogescholen en universiteiten is een professionalisering gaande, waarbij het besef doordringt dat veiligheid een randvoorwaarde is voor voortgaande internationalisering. Dat betekent onder meer focus aanbrengen en ‘proven en trusted’ relaties opbouwen met buitenlandse collega-instellingen en stageplekken. Gelijktijdig doet zich ook hier de vraag voor hoe ver de verantwoordelijkheid van de school reikt voor de veiligheid van studenten tijdens een verblijf voor stage en uitwisseling in het buitenland en wat de eigen verantwoordelijkheid van studenten en medewerkers is.

Psychologische veiligheid en welbevinden. Respondenten vragen verder aandacht voor de effecten van inkomende studenten op de sociale veiligheid aan de Nederlandse hogescholen en universiteiten. Dan gaat het onder andere om de psychologische veiligheid en welbevinden van internationale studenten en de kans dat ‘geïmporteerde conflicten’ zoals het conflict tussen Turken en Koerden, negatieve impact hebben op de verhoudingen tussen groepen studenten.

Nieuwsitem

Studenten slachtoffer van lawine

In de Franse Alpen komt begin 2017 een Nederlandse snowboarder (22) om het leven, nadat hij werd bedolven door een lawine. Twee van zijn vrienden (21 en 25 jaar) worden ook vermist. Het gaat om studenten van de Nijmeegse Studentenvereniging Navigators.⁴⁰

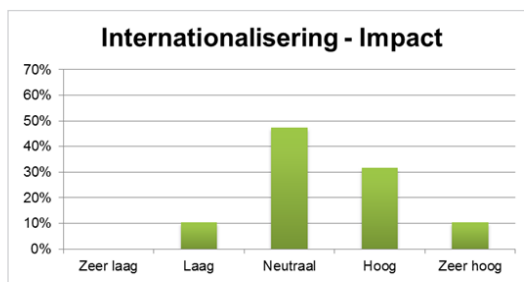
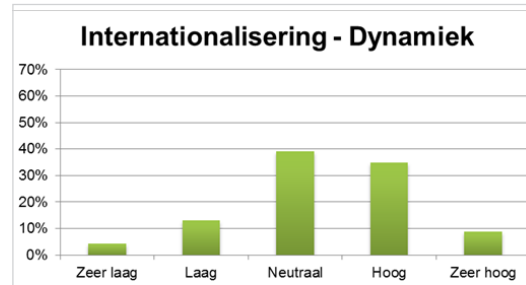
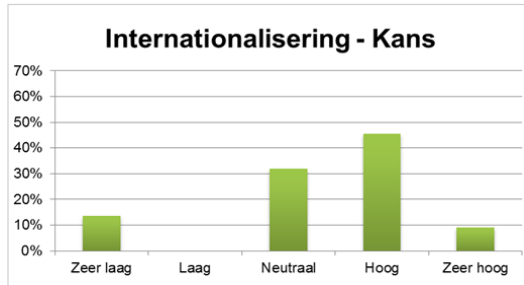
Nederlandse student slachtoffer aanslag Parijs

Een van de Nederlandse slachtoffers van de aanslagen in Parijs, volgde een opleiding in de Franse hoofdstad. Hij werd zaterdag met zware verwondingen opgenomen in het ziekenhuis en heeft een operatie moeten ondergaan. Het gaat om een jongen van pas 19 of 20 jaar oud. Hij komt uit Geleen en studeert aan de Technische Universiteit van Delft, zo hebben ‘verschillende bronnen’ bevestigd aan De Limburger.⁴¹

⁴⁰ <https://www.ad.nl/buitenland/lawineslachtoffers-in-alpen-zijn-nijmeegse-studenten-a383275e/>

⁴¹ <https://www.rtlnieuws.nl/nieuws/buitenland/student-tu-delft-zwaargewond-bij-aanslagen-parijs>

Beoordeling van kans, impact en dynamiek. Een groot deel (integrale) veiligheidscoördinatoren beoordelen de impact en de dynamiek van dreigingen binnen het thema Internationalisering als neutraal. Een kleiner, maar alsnog aanzienlijk deel van de coördinatoren, beoordelen de impact en de dynamiek als hoog. De kans dat dreigingen binnen het thema Internationalisering plaats vinden wordt voornamelijk als hoog beoordeeld. Opmerkelijk is dat enkele coördinatoren de kans als zeer laag beoordelen, terwijl geen enkele coördinator de kans als laag beoordeeld.



Figuren 11, 12 en 13:
Beoordeling kans, impact en dynamiek van Internationalisering

3.4 Integriteit

Bij integriteit gaat het om dreigingen die voortkomen uit het niet professioneel, betrouwbaar en zorgvuldig handelen, met inachtneming van de verantwoordelijkheden behorende bij functie en de geldende wet- en regelgeving en vigerende normen binnen de sector, zoals de Code Goed Bestuur van de Vereniging Hogescholen en VSNU. Voorbeelden zijn falsificatie, plagiaat, zich onterecht voordoen als (mede)auteur, niet erkennen van bijdragen van andere auteurs, belangenverstengeling, misbruik van bevoegdheden en ongewenste omgangsvormen.

Wetenschappelijke integriteit. De VNSU verzamelt sinds 2005 aangemelde en ontvankelijk verklaarde klachten rondom wetenschappelijke integriteit. In 2016 en 2017 betrof het respectievelijk zeventien en twaalf klachten.⁴² Klachten hebben betrekking op manipulatie van data, onzorgvuldige bronvermeldingen en plagiaat.

Grensoverschrijdend gedrag/ #MeToo. Het afgelopen jaar stond seksuele intimidatie nadrukkelijk op de agenda van veel organisaties. Getriggerd door de onthullingen over seksueel misbruik in Hollywood ging de hashtag #Metoo viral. Het leidde tot discussies en onthullingen over (vermeend)misbruik, tot interne onderzoeken en aanscherping van protocollen rond ongewenst gedrag. Met name in de film, culturele en ontwikkelingssector lagen organisaties onder vuur. Grensoverschrijdend gedrag kan ook in het onderwijs voorkomen, zo geeft minister van Engelshoven eind 2017 aan. Hoewel er weinig signalen uit het onderwijs bekend zijn, zou het vreemd zijn aan te nemen dat dergelijk gedrag wel in de maatschappij voorkomt en niet in het onderwijs.⁴³ De laatste jaren zijn er weinig signalen van zulk fout gedrag in andere opleidingen van het hoger onderwijs, constateert ze. "Tegelijkertijd zijn er geen redenen te veronderstellen dat het in de gehele maatschappij voorkomt en niet in het onderwijs.

Gedrag studentenverenigingen. Het gedrag van studenten lag ook in 2017 onder een vergrootglas. In het bijzonder ging het daarbij om de rol en verantwoordelijkheid van de studentenverenigingen. Zo kwam de Rotterdamse studentvereniging in januari in opspraak na onthullingen over grensoverschrijdend gedrag tijdens en ontgroening van tv-programma Rambam.⁴⁴

41 <https://www.rtlnieuws.nl/nieuws/buitenland/student-tu-delft-zwaargewond-bij-aanslagen-parijs>

42 <https://vsnu.nl/overzicht-wetenschappelijke-integriteit.html>

43 <https://www.tudelft.nl/2017/dewis/hoer-speelt-metoo-in-hoger-onderwijs/>

44 <https://www.rtlnieuws.nl/nederland/grensoverschrijdend-gedrag-bij-ontgroening-rotterdamse-studentenvereniging>

Seksueel grensoverschrijdend gedrag aan de Toneelacademie Maastricht

In november 2017 maakte een medewerker van de toneelacademie in Maastricht een melding van seksueel overschrijdend gedrag van een docent aan de school. Uit een gesprek met de studente bleek dat de docent haar op ongepaste wijze had aangeraakt en een dubbelzinnige opmerkingen had gemaakt. De Toneelacademie schorste de docent en startte een onderzoek. NOS op 3 deed zelf ook onderzoek en vond dat 29 acteurs en actrices die op de toneelacademie hadden gezeten ook negatieve ervaringen hadden gehad met dezelfde docent. Twee maanden later bleek uit onderzoek van de Volkskrant dat de academie als sinds 2005 wist van het ongepast gedrag van de docent en dat er al eerder maatregelen waren genomen. Zo mocht de docent geen studenten fysiek meer corrigeren en mocht hij ook niet meer zelf mee douchen met de studenten. Er is zelfs een aparte douche voor hem gebouwd.⁴⁵

Saxion stelt medewerker op non-actief om seksuele intimidatie

Een medewerker van Hogeschool Saxion is op non-actief gesteld omdat hij een studente seksueel geïntimideerd zou hebben. Het gaat om een incident van meer dan een jaar geleden. Pas kort geleden heeft de studente de intimidatie gemeld, mogelijk aangemoedigd door de #metoo-beweging. Studenten en personeel zijn gisteren per mail op de hoogte gesteld. Saxion laat weten dat ze een zero-tolerance beleid hanteert, en dat door het grensoverschrijdend gedrag van de medewerker “geen sprake meer was van een veilige studieomgeving”. Om privacy-redenen wil de hogeschool niet vertellen of het gaat om een docent of een medewerker met een andere functie.⁴⁶

Maatregelen om misstanden te voorkomen

De Groningse studentenvereniging Vindicat krijgt een jaar de tijd om maatregelen in te stellen die nieuwe misstanden moeten voorkomen. Zo moet er een gedragscode worden ingevoerd. Als de vereniging niet aan de eisen voldoet, verliest ze volgend jaar haar accreditatie en daarmee haar financiering. Dat maakte de commissie-Sitalsing, die de afgelopen maanden onderzoek deed naar de interne cultuur van de vereniging, vrijdag bekend. De commissie, onder leiding van oud-politiefunctaris Martin Sitalsing, werd in het najaar van 2016 ingesteld nadat Vindicat door meerdere incidenten in opspraak was gekomen. Zo kwam er een lijst naar buiten van vrouwelijke leden die ‘hete herten’ werden genoemd, en liep een aspirant-lid hersenletsel op nadat een ouderejaars op zijn hoofd was gaan staan. De Rijksuniversiteit Groningen en de Hanzehogeschool vonden dat het tijd was om de cultuur bij studentenverenigingen te veranderen.⁴⁷ In mei 2018 werd bekend dat het bestuur van Vindicat het heeft nagelaten een mishandelingsincident te melden bij de Rijksuniversiteit Groningen, een plicht die is opgenomen in de gedragscode. In reactie daarop trekken de Rijksuniversiteit Groningen en de Hanzehogeschool de bestuursbeursen voor dit schooljaar definitief in.⁴⁸

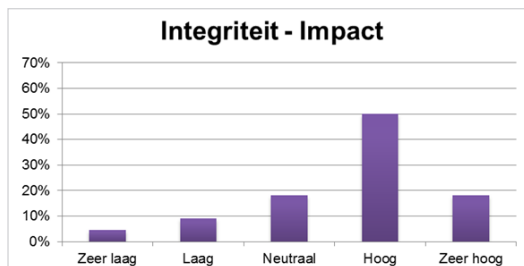
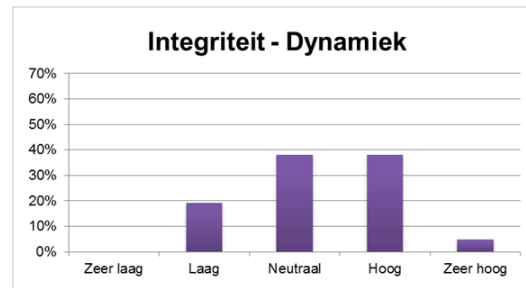
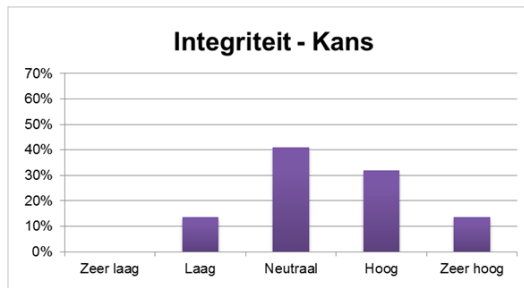
45 <https://www.volkskrant.nl/binnenland/toneelacademie-maastricht-wist-al-in-2005-van-seksueel-grensoverschrijdend-gedrag-a4557379/>

46 <https://www.advalvas.vu.nl/nieuws/saxion-stelt-medewerker-op-non-actief-om-seksuele-intimidatie>

47 <https://www.nrc.nl/nieuws/2017/07/07/vindicat-moet-binnen-jaar-voldoen-aan-voorwaarden-a1565932>

48 <https://www.nrc.nl/nieuws/2018/05/08/bestuursleden-vindicat-verliezen-beurzen-definitief-a1602223>

Beoordeling van kans, impact en dynamiek. De kans en de dynamiek van dreigingen binnen het thema Integriteit worden redelijk gelijk verdeeld door (integrale) veiligheidscoördinatoren tussen neutraal en hoog. De impact van dreigingen binnen het thema Integriteit wordt minder verdeeld beoordeeld, met de helft van de coördinatoren die de impact beoordeelt als hoog.



Figuren 14, 15 en 16:
Beoordeling kans, impact en dynamiek van Integriteit

3.5 Gebouwveiligheid

Gebouwveiligheid en BHV betreft de (brand)veiligheid van gebouwen en de BHV-maatregelen gericht op eerste hulpverlening, evacuatie en in veiligheid brengen van medewerkers, studenten en bezoekers bij calamiteiten.

Risicobeton nieuwbouwconstructies. Na het instorten van de nieuwe parkeergarage van Eindhoven Airport in mei 2017 was er landelijk veel aandacht voor gebouwen met soortgelijke vloerconstructies. Deze vloerconstructie is vooral geplaatst in grote utiliteitsgebouwen, zoals kantoren en ziekenhuizen maar ook hoger onderwijsinstellingen. In het hoger onderwijs sloten de Erasmus Universiteit Rotterdam, Saxion Hogeschool Enschede en Hogeschool Windesheim een gebouw, omdat de veiligheid van de constructie niet kon worden gegarandeerd. Ook basisscholen en middelbare scholen sloten uit voorzorg onderwijsgebouwen. De instellingen zijn veel tijd en geld kwijt met het regelen van alternatieve studieplekken, onderwijsruimtes en diverse winkels en faciliteiten.⁴⁹

Stroomstoring. Met enige regelmaat worden ook hogescholen en universiteiten geconfronteerd met stroomstoringen. Zo sluit de NHL Hogeschool in maart 2017 uit voorzorg een onderwijsgebouw, na een stroomstoring die naar verwachting 3 uur zou duren.⁵⁰ Ook de TU Delft krijgt in november 2017 te maken met een stroomstoring door graafwerkzaamheden.⁵¹ Dergelijke bedreigingen hebben impact op de continuïteit van onderwijs en onderzoek.

Brandveiligheid. Brand is een voorbeeld van een klassieke dreiging; een vraagstuk dat permanent aandacht vereist door controles op brandveiligheid en vluchtroutes, BHV-organisatie en ontruimingsoefeningen. Temeer gelet op het potentiële gevaar voor de veiligheid van studenten en medewerkers.

Zo doet zich in februari 2017 brand voor bij werkzaamheden bij het Spinozagebouw van de Radboud Universiteit. De bestuurlijke dilemma's die hiermee samenhangen worden belicht in het dilemma dat is opgesteld in opdracht van IV-HO.⁵² Na de brand in de Londense Grenfell-Tower ondervond het commerciële brandveiligheid test bedrijf Efectis een toename in het aantal vragen over brandveiligheid, met name over hoogbouw. Van dergelijke gebeurtenissen elders, kan ook impact uitgaan op hogescholen en universiteiten, bijvoorbeeld omdat er opnieuw naar veiligheidsvoorschriften wordt gekeken. Zo start de Hogeschool Rotterdam nader onderzoek naar de brandveiligheid van gevelplaten.

⁴⁹ <https://www.trouw.nl/home/scholen-met-verdachte-vloeren-blijven-gesloten-ac6c0afe/>

⁵⁰ <http://www.lc.nl/friesland/NHL-Hogeschool-dicht-vanwege-stroomstoring-in-Leeuwarden-22089456.html>

⁵¹ <https://www.omroepwest.nl/nieuws/3549596/TU-Delft-in-het-donker-door-stroomstoring>

⁵² <http://crisislab.nl/wordpress/wp-content/uploads/2017-09-11-Dilemmafiche-Brandveiligheid-Spinoza-brand.pdf>

Tijdelijke sluiting Polakgebouw Erasmus Universiteit Rotterdam

De Erasmus Universiteit Rotterdam heeft donderdagavond 19 oktober 2017 uit voorzorg besloten het Polak gebouw op campus Woudestein per direct te ontruimen en tijdelijk te sluiten. Dit om de veiligheid van studenten, medewerkers en andere gebruikers te waarborgen. Gebleken is dat in dit onderwijsgebouw eenzelfde soort vloerconstructie is gebruikt als in de parkeergarage bij Eindhoven Airport, die in mei van dit jaar gedeeltelijk instortte. Naar aanleiding van een landelijk onderzoek heeft de gemeente de universiteit gevraagd onderzoek te doen naar de vloerconstructie. Uit een bouwkundige onderzoek door een onafhankelijk ingenieursbureau is gebleken dat de veiligheid van de vloer in het gebouw niet gegarandeerd kon worden. Het CvB heeft vervolgens uit laten zoeken welke maatregelen genomen moeten worden om het gebouw zo snel mogelijk weer veilig in gebruik te nemen. De universiteit werkt aan het creëren van extra studieplekken en –mogelijkheden, om het verlies aan studieplekken in Polak te compenseren. Zo zijn de openingstijden verruimd; wordt gewerkt aan het inrichten van extra studieplekken in tijdelijke ruimtes elders op de campus en worden zo snel mogelijk verplaatst naar andere locaties. De colleges van vrijdag 20 oktober vonden reeds op alternatieve locaties plaats. Er zijn door de sluiting van Polak gebouw geen colleges uitgevallen. Studenten zijn zo goed mogelijk op de hoogte gehouden van de stand van zaken. De Bachelor Open Dag op zaterdag 21 oktober kon gewoon doorgang vinden.⁵³

Hogeschool Rotterdam sluit gebouw om Grenfell Tower-scenario te voorkomen

Na de brand in de Grenfell Tower in Londen is Hogeschool Rotterdam een onderzoek gestart naar de brandveiligheid van de eigen gevelplaten. Uit het onderzoek bleek dat in het oudste bouwdeel van de hogeschool (bouwdeel C) niet dezelfde gevelplaten waren gebruikt als in Londen, maar toch niet vast gesteld kon worden van welke brandklasse de panelen zijn. Daarom besloot Hogeschool Rotterdam om het bouwdeel te sluiten. Alle lessen en tentamens van de eerste twee dagen na het besluit kwamen te vervallen en alle studenten zijn doorverwezen naar andere locaties.⁵⁴ Na onderzoek blijkt dat ook de wanden aan de binnenkant van het gebouw niet aan de brandveiligheidsnormen voldoen. De sloop van het gebouw wordt daarom versneld uitgevoerd.⁵⁵

Stroomstoring HAN Campus Arnhem

In de ochtend van maandag 4 juli 2016 is in Arnhem een stroomstoring geweest bij netwerkbeheerder Liander. Daardoor is ook op de HAN Campus in Arnhem de stroomvoorziening uitgevallen. Tegen 14 uur waren vrijwel alle (digitale) HAN-voorzieningen weer bereikbaar. Alle tentamens gaan door, met uitzondering van 2 computertentamens bij Faculteit Economie en Management en Faculteit Gezondheid, Gedrag en Maatschappij. De betreffende studenten zijn hierover geïnformeerd.⁵⁶

Radboud controleert gebouwen op brandveiligheid

De Radboud Universiteit Nijmegen gaat al haar gebouwen controleren op brandveiligheid. De aanleiding is de brand op het dak van het Spinozagebouw afgelopen februari, die ontstond tijdens onderhoud aan een koeltoren. De portier van het Spinozagebouw bleek niet te weten hoe het brandmeldalarm geactiveerd moest worden. Doordat een technisch medewerker op een knop drukte werd weliswaar de bovenste verdieping gealarmeerd, maar ging het brandalarm niet af. Studenten in het pand werden door andere studenten die zich buiten het pand bevonden via WhatsApp gewaarschuwd. De Arbodienst concludeerde dat dit nooit had mogen gebeuren. “De Arbodienst heeft de zaak helemaal uitgezocht. Conclusie was dat de brandveiligheid van alle gebouwen van tijd tot tijd opnieuw moet worden doorlopen”, licht een woordvoerder toe. “Belangrijk aandachtspunt is voortaan dat alle verantwoordelijke medewerkers op de hoogte moeten zijn van de laatste instructies. Ook moeten de papieren instructies voor het brandalarmprotocol actueel zijn.”⁵⁷

53 <https://www.eur.nl/nieuws/update-oplossingen-voor-situatie-polak-gebouw>

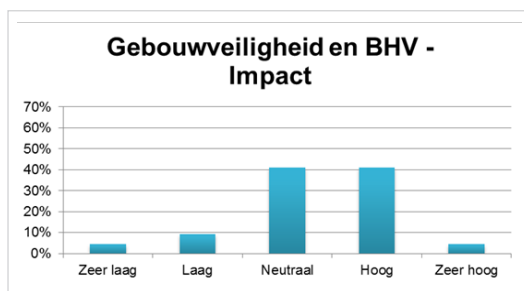
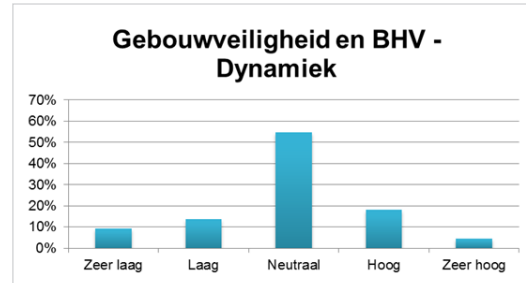
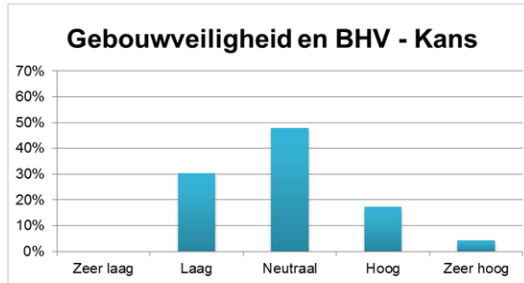
54 <https://www.volkskrant.nl/binnenland/hogeschool-rotterdam-sluit-gebouw-om-grenfell-tower-scenario-te-voorkomen-gevel-mogelijk-niet-brandveilig-a4556225/>

55 <https://www.ad.nl/rotterdam/studenten-niet-meer-terug-naar-pand-kralingsezoom-aefa6ed7/>

56 <https://www.han.nl/start/corporate/nieuws/nieuws/stroomstoring-arnhem-opge/>

57 <https://www.brandveilig.com/nieuws/radboud-universiteit-controleert-gebouwen-op-brandveiligheid-50278>

Beoordeling van kans, impact en dynamiek. De (integrale) veiligheidscoördinatoren beoordelen de kans dat er een dreiging voordoet binnen het thema Gebouwveiligheid en BHV voornamelijk als laag tot neutraal. De impact van dreigingen binnen het thema Gebouwveiligheid en BHV wordt voornamelijk beoordeeld als neutraal tot hoog. Over de dynamiek van dreigingen binnen het thema Gebouwveiligheid en BHV is weinig onenigheid, met meer dan de helft van de coördinatoren die de dynamiek van de dreigingen beoordeeld als neutraal.



Figuren 17, 18 en 19:
Beoordeling kans, impact en dynamiek van Gebouwveiligheid en BHV

3.6 Arbo en milieu

Arbo en milieu heeft betrekking op een veilige en gezonde werkomgeving voor medewerkers en studenten.

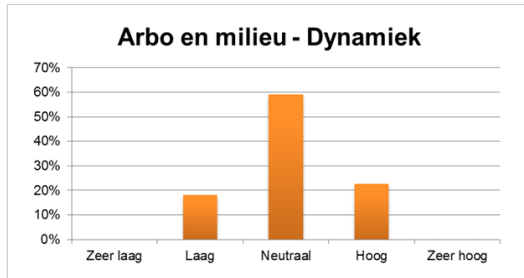
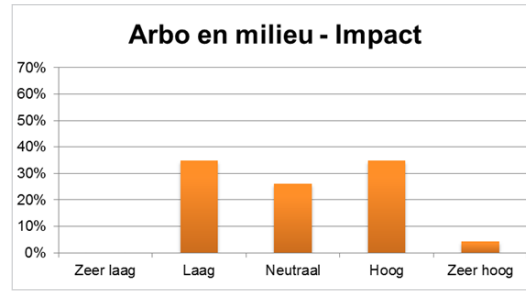
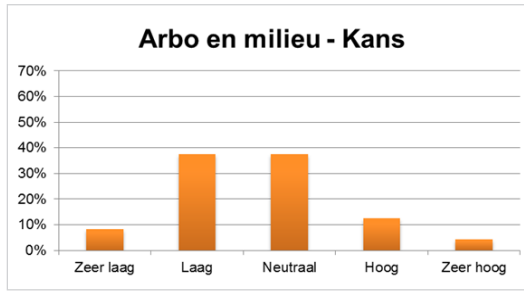
Code Rood. Het KNMI geeft tegenwoordig bij extreem weer een weeralarm ga. Daarmee informeert het KNMI met behulp van kleurcodes instanties en burgers over weersprognoses. In 2018 besloten daarop een aantal scholen uit voorzorg de deuren te sluiten en herkansing van tentamens te faciliteren om de veiligheid van studenten en medewerkers niet onnodig in gevaar te brengen.⁵⁸

Code Rood is een typisch voorbeeld van een dreiging waarachter de vraagstuk van verantwoordelijkheid schuilgaat en waar scholen zich toe moeten verhouden. Niet alleen is belangrijk dat hogescholen en universiteiten een protocol uitwerken waar in staat hoe te handelen als dit type dreiging zich voordoet. Ook helpt het de eigen rol en verantwoordelijkheid te bepalen vanuit werkgeverschap en zorg voor studenten, mede in relatie tot de eigen verantwoordelijkheid van studenten en medewerkers.

Toenemende werk en prestatiedruk: De werkdruk onder docenten in het hoger onderwijs wordt als hoog ervaren. Ook onder studenten lijkt sprake van prestatiedruk. Zo geeft in een onderzoek onder 1.800 Windesheim studenten 62% van de studenten vaak tot erg vaak prestatiedruk te ervaren tijdens hun studie, werk en sociale leven. Naast ervaren druk speelt hierin de hoge eisen die studenten aan zichzelf stellen mee. De ervaren druk om te presteren kan leiden tot psychische problemen zoals burn-out klachten en depressie.

Beoordeling van kans, impact en dynamiek. De (integrale) veiligheidscoördinatoren beoordelen de kans van dreigingen binnen het thema Arbo en milieu voornamelijk als laag tot neutraal en de dynamiek van dreigingen binnen het thema Arbo en milieu grotendeels als neutraal. Opmerkelijk is dat de coördinatoren meer zijn verdeeld over de impact van dreigingen binnen het thema Arbo en milieu. De impact wordt vaker laag en vaker hoog ingeschat dan neutraal.

⁵⁸ <https://punt.avans.nl/2017/12/code-rood-van-kracht-hoger-onderwijs-stuurt-studenten-massaal-naar-huis/>



Figuren 20, 21 en 22:
Beoordeling kans, impact en dynamiek van Arbo en milieu

3.7 Privacy en cybersecurity

Cybersecurity is de veiligheid van ICT, digitale middelen en dragers van (privacygevoelige) gegevens, zoals laptops en USB sticks. Voorbeelden van dreigingen zijn verlies van data, aantasting van de integriteit van data, identiteitsfraude, schending privacy.

Toenemende aandacht voor cybersecurity en nieuwe privacywetgeving (GDPR). Volgens SURF is er een toenemende aandacht voor cybersecurity. Diverse gezaghebbende rapporten zoals het CyberSecurityBeeld en het WRR rapport ‘De publieke kern van het internet’ onderschrijven dat beeld.⁵⁹ Verder is er, na de invoering van de meldplicht datalekken (artikel 34a, Wbp) op 1 januari 2016, vanaf 25 mei 2018 een nieuwe Europese privacyrichtlijn van kracht.⁶⁰ De wet is bedoeld om de weerbaarheid tegen nieuwe dreigingen zoals verlies van data, aantasting van privacy en cybercriminaliteit, te vergroten.

Groeiende awareness voor cybersecurity bij hogescholen en universiteiten. Binnen de instellingen is er vanuit ICT veel aandacht voor cybersecurity, wat zichtbaar wordt in securitybeleid, roadmaps, de aanstelling van specifieke functionarissen zoals de Functionaris Gegevensbescherming.^{61 62} Ook participeren hogescholen en universiteiten in jaarlijkse cyberoefeningen zoals OZON en NOZON. Ter illustratie: in oktober 2016 namen 31 onderzoeks- en onderwijsinstellingen deel aan de OZON oefening ter bevordering van de cyberweerbaarheid. Dat is volgens SURF nodig, want de bestaande crisisstructuren zijn vaak nog onvoldoende ingericht om een grote cyberdreiging het hoofd te bieden.⁶³ Tegelijkertijd geven de coördinatoren aan zorgen te hebben over de bewustwording en veilige omgang met data onder gebruikers zoals studenten, onderzoekers en docenten.⁶⁴

Tabel: deelnemers cyberoefening (N)OZON

Cyber oefening (O)ZON Deelnemende instellingen	
OZON 2016	28 instellingen (9 Goud, 5 Zilver, 14 Brons)
NOZON 2017	34 instellingen (geen verschil in niveaus)
OZON 2018	45 instellingen (Goud en Zilver)

Manipulatie data, identiteitsfraude, verwerving en openbaarmaking data en spionage vormen belangrijkste bedreigingen. Als de belangrijkste bedreigingen ziet SURF: a) het manipuleren van digitaal opgeslagen data, zoals studieresultaten en toetsmateriaal, b) identiteitsfraude, waardoor ongeautoriseerde

59 SURF, Cyberdreigingsbeeld 2016.

60 De Europese General Data Protection Regulation (GDPR) wordt in Nederland ingevoerd onder de naam Algemene Verordening Gegevensbescherming (AVG). De verordening is daarmee de opvolger van de Wet bescherming persoonsgegevens.

61 Zie bijvoorbeeld het Informatiebeveiligings- en Privacybeleid 2016-2020 van Hanze Hogeschool.

62 <https://www.fontys.nl/actueel/hub-gerats-gestart-als-corporate-information-security-office-ciso/>

63 SURF, Cybercrisoefening OZON. A gap bridging exercise.

64 Coördinatorenoverleg 16 maart 2018.

toegang tot digitale gegevens mogelijk is, waarmee cijfers kunnen worden aangepast en diefstal van tentamens kan plaatsvinden, c) verkrijgen en openbaar maken van data. Voor onderzoek worden vaak gevoelige data verwerkt en opgeslagen. Ook kunnen bepaalde onderzoeken maatschappelijk gevoelig liggen. Verder worden allerlei gevoelige data, zoals persoonsgegevens, gebruikt voor de bedrijfsvoering en d) spionage. Hogescholen en universiteiten beschikken over potentieel waardevolle data en kennis die voor criminelen en staten interessant kan zijn.⁶⁵ Verlies van dergelijke data en intellectueel eigendom wordt door organisaties als een nachtmerriescenario gezien, zo blijkt uit onderzoek door RAND. Mogelijke reputatieschade en aantasting van het vertrouwen van medewerkers, studenten en andere belanghebbenden wordt door organisaties in verschillende sectoren als een grote dreiging ervaren.⁶⁶ De grootste dreiging komt van beroeps-criminelen en statelijke actoren.⁶⁷

Bekende DDOS-aanvallen. Scholen hebben in specifieke periodes vlak voor tentamens te maken met zogenaamde Denial-of-service (DDOS) aanvallen. Deze aanvallen lijken te worden uitgevoerd door studenten. De lage complexiteit zorgt ervoor dat dergelijke aanvallen door SURFnet en de aangesloten instellingen snel gedetecteerd en geneutraliseerd kunnen worden, waardoor de impact beperkt blijft.⁶⁸

Internet of Things (IoT) Het internet der dingen is een concept, waarbij alledaagse apparaten als videocamera's, wasmachines en koelkasten zijn aangesloten op het internet, met elkaar kunnen communiceren en zelfs met een zekere autonomie kunnen functioneren. IoT-apparaten zijn vaak slecht beveiligd, ze worden vaak geleverd met een vast ingesteld wachtwoord en kwetsbaarheden worden niet of nauwelijks gepatcht. Deze apparaten kunnen worden misbruikt als toegang tot een intern systeem of worden overgenomen⁶⁹. Ook binnen het hoger onderwijs komen deze apparaten voor, van chips in proefdieren tot gebouwbeheersingssytemen.

Bring Your Own Device (BYOD) Studenten en medewerkers maken binnen hogescholen en universiteiten steeds vaker gebruik van hun eigen apparaten. Binnen dit concept van Bring Your Own Device worden privé apparaten aangesloten op systemen van de instellingen waar mogelijk gevoelige informatie is opgeslagen. Hierdoor wordt het beveiligen van gevoelige informatie steeds complexer. De uitdaging voor hogescholen en universiteiten is de informatie op een manier beveiligen waardoor alleen gemachtigde gebruikers toegang hebben.⁷⁰

Nieuwsitem

Per abuis doorsturen persoonlijke gegevens

In 2016 stuurt Hogeschool Van Hall Larenstein per ongeluk persoonlijke gegevens van 4.400 studenten door naar alle studenten van de hogeschool. Onder andere het woonadres, telefoonnummers, -mailadressen en het BSN-nummer van studenten zijn door de fout uitgelekt. De hogeschool heeft de Autoriteit Persoonsgegevens op de hoogte gesteld. Die oordeelde volgens de woordvoerder dat de school juist heeft gehandeld nadat de fout werd ontdekt⁷¹

Verlies gezondheids- en betaalgegevens

Bij een datalek bij de Erasmus Universiteit, zijn de gegevens van duizenden studenten en docenten mogelijk in verkeerde handen. Het betrof ook gevoelige gezondheids- en betaalgegevens, bijvoorbeeld over de vraag of een student allergisch is, maar ook over de aanwezigheid van tentamenvrees, dyslexie of psychische stoornissen zoals ADHD en autisme. In totaal zijn zeker 17.000 mensen getroffen door het datalek. Bij 9900 mensen werd de nationaliteit vermeld; in 5600 gevallen ging het om bank- of creditcardgegevens, en BSN- en paspoortnummers waren in 3350 gevallen aanwezig. Hoe de aanvallers precies binnenkwamen, kan de universiteit niet zeggen. Op een van de web servers trof de universiteit een achterdeurtje aan, waarmee hackers informatie van de server kunnen halen. Welke gegevens precies zijn buitgemaakt, is volgens de universiteit niet meer te achterhalen. De universiteit heeft melding gedaan bij de Autoriteit Persoonsgegevens, hetgeen sinds 1 januari verplicht is. Ook de politie is ingeschakeld.⁷²

65 SURF, Cyberdreigingsbeeld 2016.

66 RAND Europe, Investeren in cybersecurity, 2015.

67 <https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html>

68 Presentatie cyber dreigingsbeeld 2017.

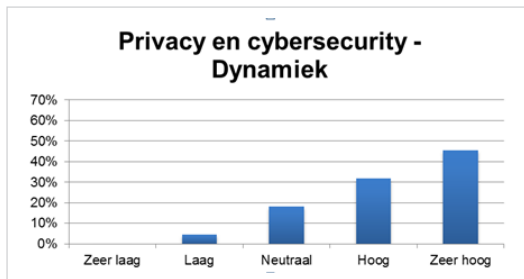
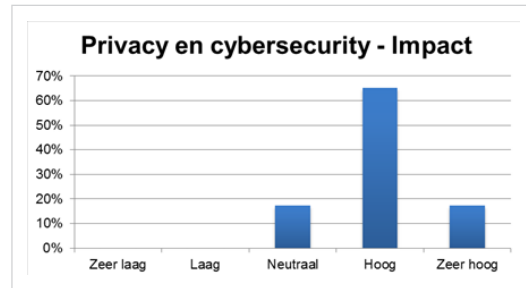
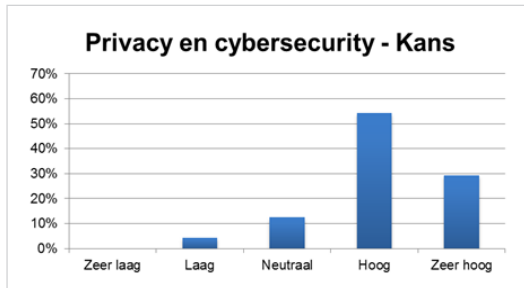
69 SURF, Cyberdreigingsbeeld 2017

70 SURF, Cyberdreigingsbeeld 2017

71 <https://www.omroepgelderland.nl/nieuws/2106621/Gegevens-4400-studenten-Van-Hall-Larenstein-op-straat>

72 <https://nos.nl/artikel/2143824-lek-erasmus-universiteit-betrof-ook-medische-gegevens-studenten.html>

Beoordeling van kans, impact en dynamiek. Het thema Privacy en cybersecurity scoort hoog op alle variabelen. De kans en impact van dreigingen binnen het thema Privacy en cybersecurity worden grotendeels beoordeeld als hoog. De verdeling van de beoordeling van de dynamiek van dreigingen binnen het thema Privacy en cybersecurity wordt steeds groter naarmate de dynamiek hoger wordt beoordeeld, met bijna de helft van de coördinatoren die de dynamiek beoordeelt als zeer hoog.



Figuren 24, 25 en 26:
Beoordeling kans, impact en dynamiek van Privacy en cybersecurity

3.8 Kennisveiligheid

Kennisveiligheid betreft de veiligheid van het intellectuele eigendom van hogescholen of universiteiten, zoals wetenschappelijke kennis, onderzoeksresultaten en innovaties. Voorbeelden van dreigingen zijn (digitale) spionage, diefstal van gegevens.

Nederlandse topsectoren populair doelwit voor economische spionage. Nederlandse topsectoren, zoals high tech, chemie, energie, water en life sciences & health vormen volgens de inlichtingendiensten een populair doelwit voor economische spionage. Daarbij neemt de complexiteit van digitale spionageactiviteiten toe en is detectie ervan lastig.⁷³

Dreiging spionage voor onderzoek hoog. SURF schat de dreiging van spionage voor het onderzoek hoog in. Dan gaat het om diefstal van intellectueel eigendom via derde partijen, controle van buitenlandse studenten door staten en het aftappen van onderzoeksdata. De dreiging is laag voor het onderwijsproces.⁷⁴

Ontbreken gedocumenteerde informatie. Beschikbare informatie over het daadwerkelijk plaatsvinden van spionageactiviteiten en impact is zeer beperkt, zo merkt SURF op, doordat er geen gedocumenteerde historie is.⁷⁵ Dat beeld bevestigen respondenten.

⁷³ SURF, Cyberdreigingsbeeld 2016.

⁷⁴ SURF, Cyberdreigingsbeeld 2016.

⁷⁵ SURF, Cyberdreigingsbeeld 2016.

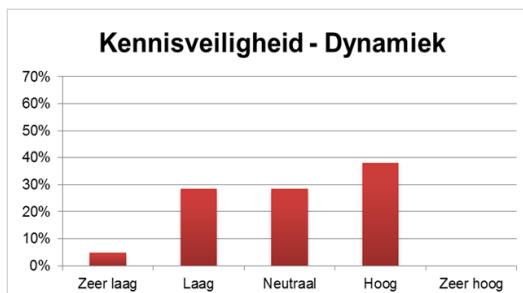
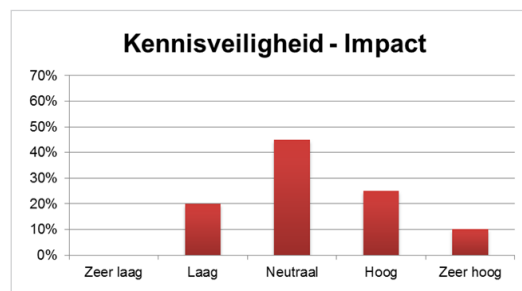
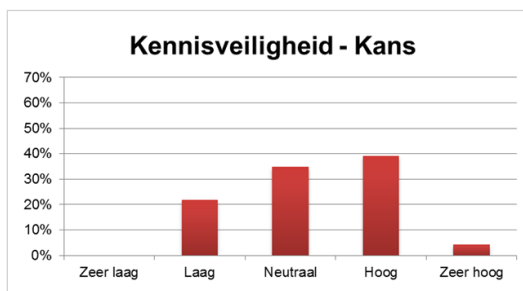
Nieuwsitem

Digitale spionage bij universiteiten

De Verenigde Staten hebben negen Iraanse hackers aangeklaagd voor digitale spionage. De hackers zouden over de hele wereld zijn binnengedrongen bij universiteiten, waaronder in Nederland. Welke Nederlandse universiteiten doelwit waren van de hackers, maakte het Amerikaanse ministerie van Justitie niet bekend. De hackers zijn niet opgepakt, maar de Verenigde Staten hebben de namen van de verdachten vrijgegeven om ze tegen te werken.

De negen hackers hebben volgens de Verenigde Staten in totaal voor 31 terabyte aan documenten en data gestolen. Bij de universiteiten gaat het om wetenschappelijke documenten en ander intellectueel eigendom. In totaal wisten de hackers achtduizend accounts van universitaire docenten binnen te dringen. In de Verenigde Staten waren 144 universiteiten doelwit. Daarbuiten zijn gegevens van 176 universiteiten in 21 landen gestolen. Naast Nederland worden onder meer Duitsland, Noorwegen, Spanje en Zweden als slachtoffer genoemd.⁷⁶

Beoordeling van kans, impact en dynamiek. De (integrale) veiligheidscoördinatoren zijn redelijk verdeeld over de beoordeling van dreigingen binnen het thema Kennisveiligheid. De kans en de dynamiek van dreigingen binnen het thema Kennisveiligheid worden het vaakst beoordeeld als hoog. De impact van dreigingen binnen het thema Kennisveiligheid wordt voornamelijk beoordeeld als neutraal.



Figuren 27, 28 en 29:
Beoordeling kans, impact en dynamiek van Kennisveiligheid

76 <https://www.nu.nl/internet/5191589/nederlandse-universiteiten-slachtoffer-van-iraanse-staatshackers.html>

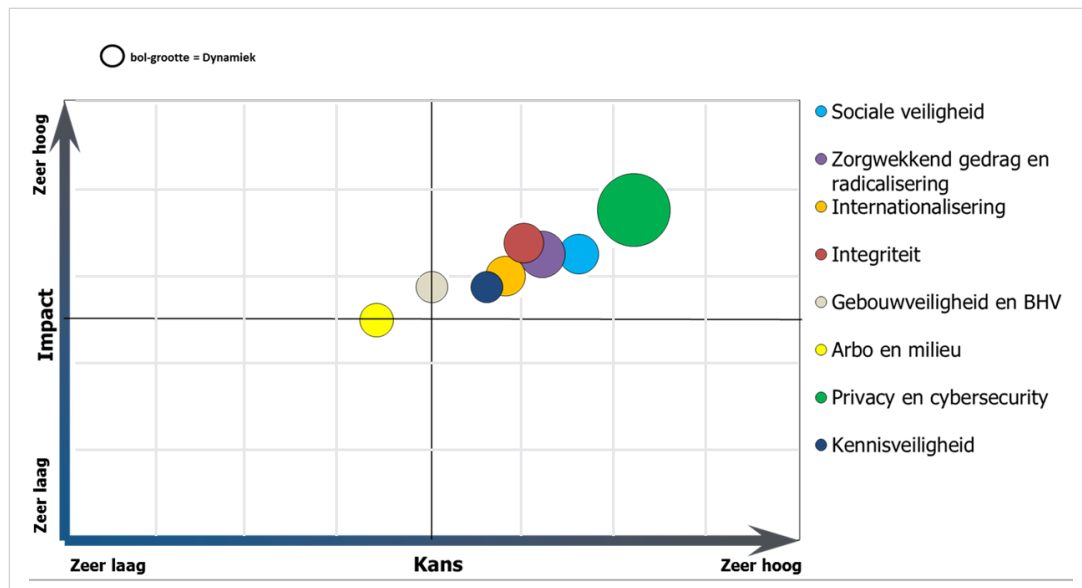
4 Dreigingsbeeld

Dit hoofdstuk bevat een overzicht en duiding van de belangrijkste dreigingen.

4.1 Integrale beoordeling dreigingen

De onderstaande matrix geeft een beoordeling van dreigingen conform de acht thema's van het programma Integrale Veiligheid Hoger Onderwijs weer. Zij doet dit aan hand van drie variabelen: de kans, de impact en de dynamiek. Het is de visualisatie van de beoordeling van de dreigingen per thema.

Zoals weergegeven in de matrix, ervaren de (integrale) veiligheidscöördinatoren in het hoger onderwijs dreigingen binnen het thema "Privacy en cybersecurity" momenteel als het meest dynamisch en de kans en de impact het grootst.



Figuur 1: Dreigingsmatrix van de thema's

Nieuwe dreigingen

Veiligheidscöördinatoren beoordelen Privacy en cybersecurity als belangrijkste dreiging. De kans en potentiële impact van de dreiging worden als hoog tot zeer hoog beoordeeld. Als mogelijke verklaring geldt de nieuwe privacy verordening AVG (met boetes), de omvang en hoge complexiteit van het vraagstuk en de mate waarin zich nieuwe ontwikkelingen voordoen. Als specifieke dreigingen komen uit onderzoek:

- Datalekken
- Manipulatie data en identiteitsfraude
- Spionage / verlies van intellectueel eigendom
- Reputatieverlies en aantasting van vertrouwen van studenten, medewerkers en andere belanghebbenden

Ook sociale veiligheid en zorgwekkend gedrag en radicalisering zijn dreigingen met een reële kans. Met name bij zorgwekkend gedrag en radicalisering signaleren respondenten de nodige dynamiek. Hier geldt, net als voor sociale veiligheid, dat de impact op de veiligheid van studenten en medewerkers groot is. Als specifieke dreigingen komen naar voren:

- Cyberpesten en –intimidatie
- Polariserende activisme dat gebruik maakt van nieuwe media
- Psychosociale en geestelijke gezondheidsproblemen/ suïcides

Bovenstaande zijn voorbeelden van nieuwe dreigingen. Dreigingen waarbinnen zich voortdurend nieuwe ontwikkelingen voordoen en waarvan de aanpak meerdere disciplines van organisaties raakt, zoals:

- Veiligheid en ICT Beveiliging
- Communicatie
- Bestuur
- Medewerkers en studenten

Dit zijn daardoor bij uitstek dreigingen waarvoor oplossingen in multidisciplinair verband gezocht moeten worden, vanuit integraliteit. Bovendien zijn oplossingen niet altijd al uitgekristalliseerd. Hoe bijvoorbeeld de weerbaarheid tegen polariserend activisme of maatschappelijke spanningen versterken of omgaan met psychosociale gezondheidsproblemen van studenten. Dat vergt soms pionieren, open vizier houden voor wat er speelt binnen de school, met elkaar casuïstiek duiden en zoeken naar handelingsperspectief.

Kwetsbaar voor incidenten

De kans dat dreigingen zich manifesteren wordt door de bevraagde coördinatoren als hoog ingeschat. Dat sluit aan bij het beeld dat oprijst uit het incidentenoverzicht (bijlage) en gesprekken met respondenten. Daaruit blijkt dat zich, op de verschillende thema's, met regelmaat incidenten voordoen bij hogescholen en universiteiten. Dan gaat het onder andere om grensoverschrijdend gedrag door studentenvereniging Vindicat, een aangifte wegens seksuele intimidatie tot een ontruiming van een onderwijsgebouw. Dat betekent niet dat de veiligheid en de veilige leer- en werkomgeving in het geding is. Wel kan hieruit worden afgeleid dat hogescholen en universiteiten kwetsbaar zijn voor incidenten. Die incidenten kunnen, afhankelijk van omvang en ernst, grote impact uitoefenen op studenten en medewerkers en de continuïteit. Dit onder druk van maatschappelijke trends als polarisatie, mediatisering en afnemende risicotolerantie.

Klassieke dreigingen

Opvallend is dat de kans en impact van meer klassieke dreigingen, zoals Arbo & milieu en gebouwveiligheid lager worden ingeschat, hoewel de potentiële impact op de veiligheid van studenten en medewerkers en de continuïteit van onderwijs hoog is. Als specifieke dreigingen worden genoemd: brand, chemicaliën ongevallen of ongevallen in laboratoria. Een mogelijke verklaring is dat dit gekende dreigingen zijn met bekende en vertrouwde beheersmaatregelen.

Dat maakt klassieke dreigingen niet minder belangrijk. De opgave ligt hier echter vooral in het goed uitvoeren en onderhouden van de beheersmaatregelen en BHV-procedures en alertheid op nieuwe situaties, zoals verandering in regelgeving, nieuwe eisen van Inspectie SZW en toezicht op brandveiligheidseisen in studentencomplexen op het campusterrein.

4.2 Specifieke dreigingen

De onderstaande tabel geeft een top-3 van specifieke dreigingen weer. De toename en grote impact van cyber-gerelateerde specifieke dreigingen als datalekken en datamanipulatie correspondeert met de hoge score op alle drie de variabelen van het thema Privacy en cybersecurity. Ook signaleren ervaren de veiligheidscoördinatoren een toename in geestelijke en psychosociale gezondheidsproblematiek. De beoordeling van nieuwe privacy wetgeving als meest impactvolle dreiging kan gerelateerd zijn aan de periode waarin de gegevens zijn bevraagd, namelijk april 2018, en de intrede van de nieuwe privacy wetgeving op 25 mei 2018.

Toenemende dreigingen (dynamiek neemt toe)	Meest impactvolle dreigingen
<ol style="list-style-type: none"> 1. Psychosociale gezondheidsproblemen 2. Datalekken 3. Geestelijke problematiek 	<ol style="list-style-type: none"> 1. Nieuwe privacy wetgeving 2. Manipulatie van data 3. Datalekken

Tabel 1: Toenemend en meest impactvolle dreigingen

De onderstaande tabel geeft de drie laagst scorende specifieke dreigingen weer. Op beide variabelen scoort grensoverschrijdend gedrag van studentenverenigingen het laagst. Dit kan worden verklaard doordat hogescholen en universiteiten het grensoverschrijdend gedrag primair als verantwoordelijkheid van de studentenverenigingen ziet (en niet of minder als de verantwoordelijkheid van de school). Deze dreiging wordt als minst impactvol gezien. Ook dreigingen als brand en terrorisme worden als afnemend ingeschat. Geïmporteerde conflicten en problemen met bouwconstructies worden als weinig impactvol beoordeeld.

Afnemende of stabiliserende dreigingen (dynamiek neemt af)	Minst impactvolle dreigingen
Grensoverschrijdend gedrag studentenverenigingen	Grensoverschrijdend gedrag
Brand	Geïmporteerde conflicten
Terrorisme(dreiging)	Veiligheid van bouwconstructies

Tabel 2: Afnemend/stabiel en minst impactvolle dreigingen

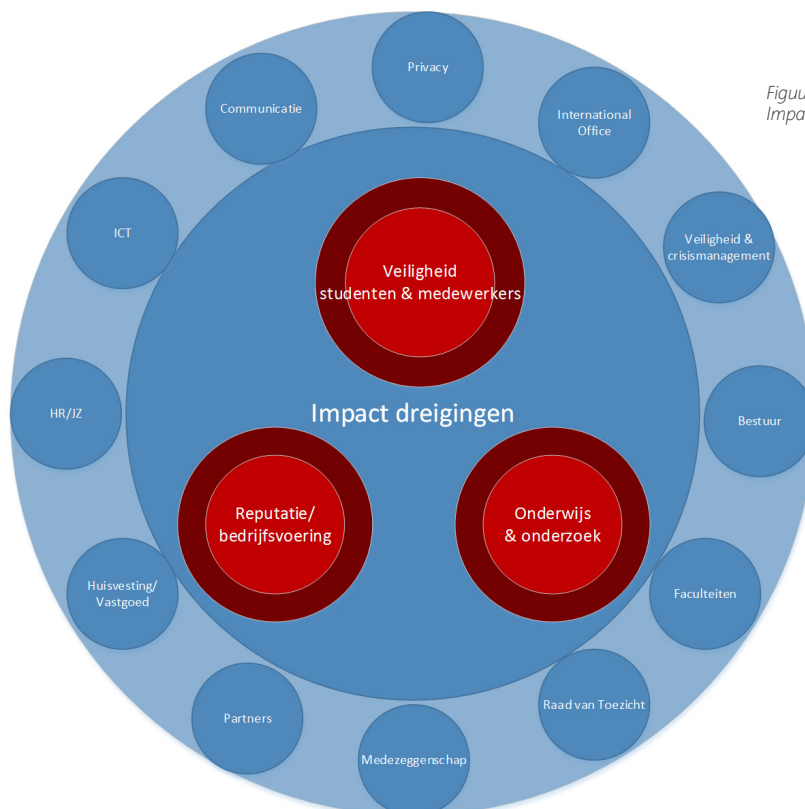
4.3 Impactgebieden dreigingen

Dreigingen kunnen op meerdere gebieden impact hebben. Zij kunnen:

1. de veiligheid van studenten en medewerkers aantasten
2. de integriteit en continuïteit van onderwijs en onderzoek bedreigen
3. reputatie en bedrijfsvoering schaden.

Een voorbeeld: verlies van data kan impact uitoefenen op studenten, de integriteit van onderzoeksgegevens en gelijktijdig de bedrijfsvoering verstoren.

In de figuur zijn deze impactgebieden (rood gemarkeerd) weergegeven. Voor het beheersen van schadelijke impact kan een aanpak vanuit meerdere disciplines en expertises zoals HR, communicatie en veiligheid, vereist zijn. Een indicatieve set van disciplines is opgenomen in de buitenste ring. Het bepalen van impact en van benodigde expertise en disciplines is onderdeel van een integrale respons.



Figuur 1: Impactgebieden en disciplines

5 Weerbaar tegen dreigingen: vier reflectievragen voor de bestuurstafel

Dit dreigingsbeeld geeft een actueel, landelijk beeld van dreigingen die spelen voor hogescholen en universiteiten. De uitkomsten betekenen niet automatisch dat dit de dreigingen zijn waar uw instelling mee te maken heeft. Dat kan per instelling verschillen. Mogelijk heeft u al maatregelen getroffen en zijn de belangrijkste dreigingen in beeld. Mogelijk ook niet. Duidelijk is wel dat voor iedere instelling dit dreigingsbeeld als vertrekpunt kan dienen om het bestuurlijke gesprek over dreigingen te voeren.

Om die stap van ‘papier rapportage’ naar de praktijk te faciliteren en het bestuurlijke gesprek over veiligheid binnen de hogescholen en universiteiten te bevorderen, formuleren we vier reflectievragen.

I Zicht op dreigingen

Bestuurlijke vraag 1: Hoe verhoudt het dreigingsbeeld zich tot de dreigingen waarop onze hogeschool of universiteit zich voorbereid? Staan nieuwe dreigingen op onze bestuurlijke agenda?

Hoe verhouden de uitkomsten van het dreigingsbeeld zich tot de dreigingen binnen onze instelling? Hoe is onze organisatie voorbereid op de geïdentificeerde dreigingen? Waar zitten nog kwetsbaarheden en wat betekent dat voor onze aanpak? Zijn er dreigingen waarvan we vinden dat we daar expliciet niet aanvullend op willen voorbereiden?

II Sturing informatie

Bestuurlijke vraag 2: Wat weten we over onze ‘eigen’ dreigingen? Welke sturingsinformatie hebben we?

Niet alle hogescholen en universiteiten brengen op een gestructureerde manier de beschikbare informatie over dreigingen, incidenten en de afhandeling bijeen. Daardoor blijft onduidelijk wat de omvang en ernst van dreigingen is, hoewel er vaak wel veel (gefragmenteerde) informatie beschikbaar is, bijvoorbeeld in incidentrapportages, meldingen bij ICT of vertrouwenspersonen en in de hoofden van medewerkers. Om gefundeerde afwegingen over veiligheid te maken, is die informatie essentieel. Advies is dan ook om die informatie periodiek, bijvoorbeeld jaarlijks, te verzamelen en met een multidisciplinaire groep medewerkers van verschillende disciplines (bestuur, veiligheid, onderwijs, ICT, vertrouwenspersonen, communicatie) te duiden. Die intelligence dient als waardevolle sturingsinformatie: om keuzes te maken en prioriteiten te stellen.

Dreigingen zijn dynamisch. Ze veranderen of blijven gelijk onder invloed van bepaalde omstandigheden (door andere, betere beheersmaatregelen, verandering in perceptie, andere ambities). Om die reden adviseren we hogescholen en universiteiten het eigen dreigingsprofiel periodiek te actualiseren. Daarbij hoort beantwoording van vragen als:

- Zijn ‘onze’ dreigingen nog dezelfde als twee jaar geleden?
- Zijn er omstandigheden waardoor het dreigingsprofiel is veranderd, bijvoorbeeld door nieuwe strategische ambities (meer internationale uitwisseling, uitbreiding van laboratoria, nieuwbouw, etc.)?
- Zijn bestaande maatregelen nog voldoende toegespitst op de dreigingen? Moet er iets af, of juist bij?

III Preparatie

Bestuurlijke vraag 3: Hoe bereiden wij ons voor op dreigingen: reactief, bewust accepteren van dreigingen, beleid maken, flexibel reageren? Hoe verbinden we veiligheid aan onze bredere strategische doelstellingen?

Hogescholen en universiteiten bereiden zich in praktijk verschillend voor op dreigingen, van proactief en planmatig tot ad hoc. Dat is begrijpelijk en ook terecht, gelet op de verschillen in onder meer schaalgrootte, locaties, activiteiten en ambities tussen de instellingen. Er is geen ‘one size fits all’. Bovendien vraagt iedere dreiging iets anders. Structurele dreigingen van een aantoonbare omvang met potentieel grote impact, zoals cyberveiligheid, vergen een beleidsmatige aanpak. Meer uitzonderlijke dreigingen zoals sluimerende polarisatie tussen groepen bieden juist ruimte voor anticiperen en alert reageren als het zich manifesteert.

Sommige dreigingen (terrorisme, spionage) zijn dermate uitzonderlijk, dat investeren in preventie onevenredig veel tijd, geld en capaciteit kost. In dergelijke gevallen is wijs beleid: het bewust accepteren van die specifieke dreiging. Zeker indien er geen concrete aanwijzingen zijn van een dreigende aanslag of spionage activiteiten.

Weerbaar tegen dreigingen: voorstelbare acties

Type dreiging	Actierepertoires
Uitzonderlijke dreigingen (terrorisme, spionage)	Weloverwogen accepteren van dreigingen
Structurele dreigingen, grote impact (cyberveiligheid, gebouwveiligheid)	Investeren in (preventief) beleid en awareness
Dynamische, nieuwe dreigingen (zorgwekkend gedrag, online bedreigingen, polarisatie)	Investeren in alert en flexibel reageren (inrichten casuoverleg, expertisenetwerk, integraal crisismanagement)

De kernvraag is hoe ver uw instelling voorbereid wil zijn en wat is uw bestuurlijke ambitie op veiligheid? Gaat uw instelling dan voor het maximaal haalbare of alleen voor wat vanuit wet- en regelgeving verplicht is (compliance)? En hoe stelt u zeker dat u daarin groei doormaakt en naar een bepaald volwassenheidsniveau toegroeit?



Bestuurlijke vraag 4: Hoe is ons toezicht op veiligheid ingericht? Welke expertise kunnen we inschakelen om de weerbaarheid tegen specifieke dreigingen te bevorderen?

Dreigingen vragen, zeker in de huidige tijd (snelle veranderingen, afnemende risicotolerantie, complexiteit), structureel aandacht. Een heldere governance draagt bij aan het bevorderen van de weerbaarheid. Wat is de rol en betrokkenheid van het College van Bestuur? Is er een periodiek integraal veiligheidsoverleg en vinden verschillende disciplines (ICT, Communicatie, International Office, Veiligheid) elkaar? Hoe wordt de Raad van Toezicht geïnformeerd? Welke expertise hebben we nodig om dreigingen te weerstaan en is die expertise in huis?

Integrale aanpak van dreigingen

Dimensies	Toelichting
1.	Integraal: van preventie tot nazorg (gehele veiligheidsketen)
2.	Integraal, vanuit alle benodigde disciplines (ICT, veiligheid, communicatie, HR, JZ, Bestuur) en thema's
3.	Integraal, van bestuur tot werkvloer. Op alle niveaus binnen de organisatie: studenten en medewerkers, faculteiten, bestuur, Raad van Toezicht
4.	Integraal: met externe partners, zoals gemeente, politie, collega-instellingen en bedrijven (elke partij heeft immers haar kennis, expertise, informatie of netwerk)



6 Tot slot

De kerntaak van hoger onderwijsinstellingen is het geven van goed onderwijs. Een veilig onderwijsklimaat draagt daar aan bij. Waar studenten, medewerkers en derden zich veilig voelen ontstaat een goede plek om te leren. Het dreigingsbeeld hoopt een bijdrage te leveren aan het veilige onderwijsklimaat. Door u mogelijk op onbekende dreigingen te wijzen of door onderwijsinstellingen juist de overtuiging te geven dat ze op de goede weg zijn. Wij wensen u veel succes met de toepassing in uw eigen onderwijsorganisatie.

Juni 2018

COT Instituut voor Veiligheids- en Crisismanagement

Laurens van der Varst

Nico Kaptein

Frank Kuipers

Nils Dalmeijer

Bijlage 1 Beschrijving thema's

Het dreigingsbeeld is opgebouwd rond acht thema's van IV-HO. De acht thema's staan hieronder toegelicht.

Sociale veiligheid is het ontbreken van (ervaren) aantasting van de veiligheid en fysieke integriteit van personen. Voorbeelden van sociale onveiligheid: fraude, agressie en geweld, stalking, (seksuele) intimidatie, pesten/ discriminatie, bedreiging, polarisatie, psychische problematiek, suicide, interculturele, etnische en religieuze verschillen en hieruit voortvloeiende risico's en niet-integer handelen (zoals belangenverstremming, misbruik bevoegdheden, ongewenste omgangsvormen).

Zorgwekkend gedrag en radicalisering. Concrete gedragingen of signalen die wijzen op de bereidheid geweld te gebruiken of hiermee te dreigen. Die bereidheid kan voorkomen uit bijvoorbeeld ideologische overtuigingen, geestelijke problematiek of anderszins. Voorbeelden zijn huiselijk geweld, radicalisering, bedreigingen, agressie en geweld.

Internationalisering. Veiligheidsrisico's die verbonden zijn aan internationale mobiliteit van studenten en medewerkers van hogescholen en universiteiten, in het kader van uitwisselingsprogramma's, stages en onderzoeken. Hierbij gaat het zowel om uitgaande als inkomende mobiliteit. Voorbeelden uitgaande mobiliteit: geweld/terrorisme, natuurramp of epidemie, diefstal, gezondheids- en psychische problemen. Voorbeelden inkomende mobiliteit: gezondheids- en psychische problemen, diefstal, interculturele botsingen en spanningen.

Integriteit. Professioneel, betrouwbaar en zorgvuldig handelen, met inachtneming van de verantwoordelijkheden behorende bij je functie en de geldende wet- en regelgeving en vigerende normen binnen de sector zoals de Code Goed Bestuur van de Vereniging Hogescholen en VSNU en de eigen organisatie. Voorbeelden van risico's: falsificatie, plagiaat, zich onterecht voordoen als (mede)auteur, niet erkennen van bijdragen van andere auteurs, datalekken, verduistering, belangenverstremming, misbruik van bevoegdheden en ongewenste omgangsvormen.

Gebouwveiligheid. De veiligheid van gebouwen en de BHV maatregelen gericht op eerste hulpverlening, evacuatie en in veiligheid brengen van medewerkers, studenten en bezoekers bij calamiteiten.

Arbo en milieu heeft betrekking op een veilige en gezonde omgeving voor medewerkers en studenten. Hierbij gaat het om onderwerpen als een gezonde werkplek, verzuim, preventie, ongewenst gedrag, werkdruk, gevaarlijke stoffen, machineveiligheid en arbeidsrisico's.

Privacy en cybersecurity. Cybersecurity richt zich op de bescherming tegen cybercrime en datalekken en op de continuïteit in de bedrijfsvoering en Privacy is een individueel recht.

Kennisveiligheid. De veiligheid van het intellectuele eigendom van hogescholen/universiteiten: de kennis, vorderingen en resultaten van onderzoeken en innovaties. Risico's die spelen bij wetenschappelijk onderzoek en innovaties zijn: (digitale) spionage, diefstal van gegevens of social engineering door inlichtingendiensten of commerciële organisaties.

77 Het programma IV-HO hanteert in totaal tien thema's. Twee van de tien thema's zijn niet opgenomen als thema's van dit dreigingsbeeld: thema's Integrale veiligheid en Crisismanagement. Zie: <https://www.integraalveilig-ho.nl/thema/>

Bijlage 2 Overzicht incidenten 2017 – 2018

Datum	Beschrijving	Thema	Instelling	Link
5 jan 2017	Uit onderzoek blijkt dat zelfmoord de nummer twee doodsoorzaak onder studenten is.	Sociale veiligheid	Hoger onderwijs in het algemeen	https://www.nporadio1.nl/homepage/2651-heel-veel-studenten-zijn-eenzaam-en-somber-en-denken-na-over-zelfmoord
12 jan 2017	Een medewerker van de Erasmus Universiteit Rotterdam valt van de trap. Er is mogelijk opzet in het spel.	Gebouwveiligheid en BVH Zorgwekkend gedrag en radicalisering Arbo en milieu	Erasmus Universiteit Rotterdam	https://www.ad.nl/rotterdam/medewerker-erasmus-universiteit-gewond-mogelijk-van-trap-geduwd-aa2a7c2e/
14 feb 2017	Er breekt een grote brand uit in het Spinozagebouw van de Radboud Universiteit Nijmegen. De oorzaak van de brand is onduidelijk.	Gebouwveiligheid en BHV	Radboud Universiteit Nijmegen	https://nos.nl/artikel/2158208-grote-brand-bij-radboud-universiteit-nijmegen.html
27 feb 2017	Een student van de Hogeschool InHolland hackt in het schoolsysteem om tentamens te verkrijgen.	Privacy en cybersecurity	Hogeschool InHolland	https://www.rijnmond.nl/nieuws/152272/Student-InHolland-hackte-voor-tentamens
8 maart 2017	Studenten uit Nijmegen komen om bij een lawine in de Franse Alpen. De instellingen waar de studenten studeren organiseren een persconferentie.	Internationalisering	Radboud Universiteit Nijmegen Hogeschool van Arnhem en Nijmegen	https://www.ad.nl/buitenland/lawineslachtoffers-in-alpen-zijn-nijmeegse-studenten-a383275e/
15 mei 2017	Na het ontstaan van giftige dampen door een brand in het laboratorium, wordt de Hogeschool Saxion ontruimd.	Gebouwveiligheid en BHV	Hogeschool Saxion	http://www.rtvooost.nl/nieuws/268868/saxion-hogeschool-in-enschede-ontruimd-na-vrijkomen-giftige-dampen-update#
23 mei 2017	In de media wordt bericht dat studenten van de Universiteit van Amsterdam tot 10.000 gebruikssaccount van Blackboard en examenvragen konden achterhalen.	Privacy en cybersecurity	Universiteit van Amsterdam	https://tweakers.net/nieuws/125001/gebreken-in-uva-blackboard-gaven-toegang-tot-10000-accounts.html
12 juni 2017	In de media wordt bericht dat studenten van de Universiteit van Amsterdam tot 10.000 gebruikssaccount van Blackboard en examenvragen konden achterhalen.	Privacy en cybersecurity	Universiteit Utrecht	https://www.dub.uu.nl/nl/nieuws/persoon-dood-gevonden-ornsteinlaboratorium
4 sep 2017	Hogeschool Rotterdam ontruimt na een brand in de liftschacht.	Gebouwveiligheid en BHV	Hogeschool Rotterdam	https://www.ad.nl/rotterdam/studenten-op-straat-na-korte-brand-bij-hogeschool-rotterdam-a413f560/
19 okt 2017	De vloerconstructie van het Polak gebouw blijkt dezelfde vloerconstructie te hebben als de ingestorte parkeergarage in Eindhoven. Het gebouw wordt ontruimd.	Gebouwveiligheid en BHV	Erasmus Universiteit Rotterdam	https://www.rtlnieuws.nl/nederland/gebouw-erasmus-universiteit-ontruimd-om-instortingsgevaar
26 okt 2017	Ook een gebouw van Hogeschool Saxion heeft dezelfde constructie als de parkeergarage in Eindhoven. Het gebouw wordt gesloten.	Gebouwveiligheid en BHV	Hogeschool Saxion	https://www.nu.nl/binnenland/4980752/gebouw-hogeschool-saxion-deels-gesloten-gevaarlijke-constructies.html
2 nov 2017	Toneelschool Maastricht schorst docent vanwege ongewenst (seksueel) gedrag. Uit onderzoek blijkt dat meer studenten negatieve ervaring met de docent hebben gehad. Een deel van de studenten beschuldigt de leraar van machtsmisbruik en seksuele intimidatie.	Integriteit Zorgwekkend gedrag en radicalisering	Toneelschool Maastricht	https://nos.nl/op3/artikel/2200996-acteurs-over-toneel-docent-maastricht-jarenlange-seksuele-intimidatie.html

Datum	Beschrijving	Thema	Instelling	Link
21 nov 2017	Een student doet aangifte wegen seksuele intimidatie tegen een medewerker van de Hogeschool. De medewerker wordt op non-actief gesteld.	Integriteit Zorgwekkend gedrag en radicalisering	Hogeschool Saxion	https://www.rtlnieuws.nl/nederland/medewerker-hogeschool-op-non-actief-om-ontucht
1 dec 2017	De Avans in Den Bosch heeft last van een grote DDoS-aanval.	Privacy en cybersecurity	Hogeschool Avans Den Bosch	https://punt.avans.nl/2017/12/avans-weerstaat-vrijdagochtend-twee-ddos-aanvallen/
11 jan 2018	Hogeschool Rotterdam sluit uit voorzorg zijn gebouwen voor nadere inspectie van de gevelplaten.	Gebouwveiligheid en BHV	Hogeschool Rotterdam	https://www.nu.nl/binnenland/5082098/hogeschool-rotterdam-sluit-gebouw-in-verband-met-brandgevaar-gevelplaten.html
18 jan 2018	Een verwarde man steek twee studenten neer op de Campus van Universiteit Wageningen.	Zorgwekkend gedrag en radicalisering	Universiteit Wageningen	https://nos.nl/artikel/2212506-twee-gewonden-bij-geweldsincident-op-universiteitscampus-wageningen.html
3 april 2018	Hogeschool Utrecht wordt ontruimd wegens brand na een ontploffing in een zuurkast.	Gebouwveiligheid en BHV	Hogeschool Utrecht	https://www.nu.nl/utrecht/5204648/gebouw-hogeschool-utrecht-tijdelijk-ontruimd-vanwege-brand.html
4 april 2018	Man met een nep wapen wordt aangehouden bij de Haagse Hogeschool	Zorgwekkend gedrag en radicalisering	Haagse Hogeschool	https://www.omroepwest.nl/nieuws/3611643/Man-met-nepwapen-aangehouden-bij-Haagse-Hogeschool
30 april 2018	Universiteit Twente wordt slachtoffer van een phishing aanval	Privacy en cybersecurity	Universiteit Twente	https://www.tubantia.nl/enschede/ut-getroffen-door-phishingaanval-aaa0fc3c/
1 mei 2018	Duizenden gegevens van studenten lekken uit na een datalek bij Hogeschool Saxion	Privacy en cybersecurity	Hogeschool Saxion	https://nos.nl/artikel/2229926-gegevens-studenten-hogeschool-saxion-op-straat-door-datalek.html
1 mei 2018	Studentenvereniging Vindicat komt wederom negatief in het nieuws na een niet gemelde mishandeling. De bestuursbeurzen worden ingetrokken.	Zorgwekkend gedrag en radicalisering	Rijksuniversiteit Groningen	https://www.rtlnieuws.nl/nederland/weer-mishandeling-bij-studentenvereniging-vindicat-incident-niet-gemeld



Bijlage 3

Coördinatoren­groep en respondenten

De coördinatoren­groep is in het kader van dit project bijeen geweest op:

1. 16 maart: Onderwerp: trends en ontwikkelingen
2. 26 april: Onderwerp: uitkomsten online survey
3. 24 mei: Onderwerp: rapportage dreigingsbeeld

De volgende personen zijn lid van de coördinatoren­groep: Rene Ritzen (Universiteit Utrecht), Paul Goossens (Hogeschool Rotterdam), Daan van den Tillaar (Hogeschool van Arnhem en Nijmegen), Bart van den Heuvel (Maastricht University), Raoul Vernede (Wageningen University), Anita Polderdijk (Hogeschool Windesheim), C.S. Vos (Universiteit Utrecht), Wilma Mossink (Hogeschool Van Hall Larenstein), Peter Wurtz (Universiteit van Amsterdam), Rogier Ragatlie (EUR), Timo Stortenbeker (Hogeschool InHolland), M.M. Boumans (Avans), Marjon Gielisse (De Haagse Hogeschool), Michael Mehrow (Hogeschool Windesheim), Bastiaan van Vliet (SURF/programma IV-HO), Klaasjan Boon (SURF/programma IV-HO) en Charlie van Genuchten (SURF/programma IV-HO).

De volgende deskundigen zijn geraadpleegd: Edwin Bakker (Hoogleraar Terrorisme en Contraterrorisme), Ira Helsloot (Hoogleraar Besturen van Veiligheid), Marnix Eysink Smeets (Lector Publiek Vertrouwen in Veiligheid), Wouter Stol (Lector Cybersafety en Hoogleraar Politiestudies), Sjaak Khonraad (Lector Integrale Veiligheid), Theo van Kouterik (OCW), Dirk Haaksman (Nuffic), Beer Schröder (Nuffic), Aldert Jonkman (Vereniging Hogescholen).

Bijlage 4

Achtergrondinformatie dreigingen

- Aon, Terrorism and Political Violence Risk Map 2017.
- AIVD, Jaarverslag 2017, 2018.
- CBS, Het mysterie van de verdwenen criminaliteit, 2018.
- Clingendael, Strategische Monitor 2017.
- Crisislab – Bestuurlijke Veiligheidsdilemma's Hoger Onderwijs
<http://crisislab.nl/bestuurlijke-veiligheidsdilemmas-in-hoger-onderwijs/>
- DUO, Buitenlandse reizen in het voortgezet onderwijs, 2018.
- Helsloot, Vlagsma & Kraaijenbrink - Risk Analysis of Higher Education Institutions
<http://crisislab.nl/wordpress/wp-content/uploads/Risk-analysis-HEIs.pdf>
- Hogeschool Rotterdam – Jaarverslag Integrale Veiligheid
<https://www.hogeschoolrotterdam.nl/hogeschool/nieuws/jaarverslag-integrale-veiligheid/>
- Nationaal Cyber Security Centrum, Cyber Security Beeld Nederland, 2017.
- NCTV, Dreigingsbeeld Terrorisme Nederland (DTN), 2018.
- Programma Integrale Veiligheid Hoger Onderwijs, Stappenplan integrale veiligheidsrisicoprofiel (met groslijst aan veiligheidsrisico's in het hoger onderwijs): <https://integraalveilig-ho.nl/wp-content/uploads/Stappenplan-integrale-veiligheid-risicoprofiel.pdf>
- Raad van Advies, Advies over veiligheid in het hoger onderwijs.
- RAND Europe, Investeren in cybersecurity, 2015.
- Slovic, The perception of risk, 2016.
- SURF, Cybercrisisoefening OZON. A gap bridging exercise.
- SURFnet – Cyberdreigingsbeeld Hoger Onderwijs 2016, 2017.
<https://www.integraalveilig-ho.nl/instrument/cyberdreigingsbeeld-hoger-onderwijs/>
- Regionaal risicoprofiel veiligheidsregio

Over het COT

Het COT helpt publieke; semi-publieke en private organisaties bij het opstellen en reviewen van veiligheidsvisies, crisisplannen, inrichten van crisisorganisaties, trainingen en oefeningen en alle andere voorkomende vraagstukken op het gebied van veiligheid en crisismanagement. Terugkerende kenmerken van crisismanagement binnen het onderwijs zijn de sterk gevoelde zorg voor studenten en medewerkers, het belang van de voortgang van het onderwijsproces en de uitdaging van decentrale autonomie versus benodigde centrale regie. Onze trainers en adviseurs zijn gewend te schakelen tussen diverse organisatieniveaus.

Het COT adviseerde diverse onderwijsinstellingen rond gevoelige kwesties als terrorismeverdachten, een datalek, mogelijke grootschalige fraude en een bestuurlijke crisis. Wij zijn trots op het feit dat wij een langdurig partnerschap hebben met meer dan vijftientig gerenommeerde hogescholen, universiteiten en ROC's.

Net als SURF en het programma Integrale Veiligheid Hoger Onderwijs, vindt het COT kennisvermeerdering en kennisontsluiting belangrijk. Daarom organiseren wij themabijeenkomsten en plaatsen wij op LinkedIn regelmatig posts over ontwikkelingen in ons vakgebied. Zie o.a. onze speciale LinkedIn-groep over crisismanagement in het onderwijs en onze posts over veiligheid en het onderwijs.

Meer informatie: www.cot.nl of cot@cot.nl



Over COT

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismangement en is onderdeel van Aon Global Risk Consultants. Ons werkteerrein strekt zich uit van vraagstukken over veiligheidsambities tot de voorbereiding en reactie op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT opereert vanuit Rotterdam en is een volledige dochteronderneming van Aon Nederland.

Over Aon

Aon plc (NYSE:AON) is een toonaangevende wereldwijde dienstverlener op het gebied van risk, retirement en health. Aon analyseert de personele risico's en bedrijfsrisico's, geeft passend risicoadvies, zorgt voor de (financiële) oplossing én is er als een incident de bedrijfscontinuïteit bedreigt. Zo helpen wij klanten succesvol te ondernemen.

Aon heeft in Nederland 8 vestigingen met 1.540 medewerkers en in 120 landen meer dan 50.000 collega's. Ga voor meer informatie naar www.aon.nl.

© 2018 Aon Nederland

Alle rechten voorbehouden. Niets uit deze rapportage mag worden veeveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Aon.

