



>Retouradres Postbus 16375 2500 BJ Den Haag

Ontvangen: 11-5-2023

2023/019++vt

Universiteit Leiden
T.a.v. het College van Bestuur
Postbus 9500
2300 RA LEIDEN

**Hoger Onderwijs en
Studiefinanciering**
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
38325432

Bijlagen
1

Datum 11 mei 2023
Betreft Besluit macrodoelmatigheid wo-bacheloropleiding Cybersecurity & Cybercrime

Als u belang hebt bij dit besluit, dan kunt u hiertegen binnen 6 weken, gerekend vanaf de verzenddatum, bezwaar maken. Stuur uw bezwaarschrift naar DUO, Postbus 30205, 2500 GE Den Haag. U kunt uw bezwaar ook digitaal indienen op www.bezwaarschriftenocw.nl.

Geacht bestuur,

Met de brief van 20 maart 2023, door de Commissie Doelmatigheid Hoger Onderwijs (hierna: CDHO) ontvangen op 20 maart 2023, hebt u mij het voornemen voorgelegd om de wo-bacheloropleiding Cybersecurity & Cybercrime als bekostigde opleiding te verzorgen in Den Haag.

Advies CDHO

De CDHO heeft mij bij brief van 17 april 2023, kenmerk 2023/019, positief geadviseerd over uw aanvraag. Dit advies, dat integraal deel uitmaakt van dit besluit, treft u hierbij aan.

Besluit

Gelet op het bovengenoemd advies van de CDHO, het bepaalde in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (hierna: WHW) en in de Regeling macrodoelmatigheid hoger onderwijs (hierna: Regeling), heb ik besloten in te stemmen met uw voornemen om de wo-bacheloropleiding Cybersecurity & Cybercrime als bekostigde opleiding te verzorgen in Den Haag. Met toepassing van artikel 6.2, derde lid, van de WHW, beperk ik mijn instemming tot de voltijdvariant.

Beoordelingskader

De wettelijke grondslag voor mijn besluitvorming is gelegen in artikel 6.2 van de WHW. Voorts is de Regeling leidraad geweest voor mijn afwegingen.

Motivering

Overeenkomstig het advies van de CDHO concludeer ik dat uw aanvraag, voldoet aan de criteria a en b van artikel 4, eerste lid, van de Regeling. Voor de nadere motivering verwijs ik u naar het genoemde advies van de CDHO.

Croho-procedure

Ingevolge artikel 6.2, negende lid van de WHW vervalt dit besluit indien de opleiding niet binnen tien maanden na dagtekening van dit besluit is geregistreerd in het Croho. Registratie binnen die termijn is niet eerder mogelijk dan nadat de NVAO een positief besluit heeft genomen in het kader van de toets nieuwe

opleiding. In verband met de geldigheidsduur van dit besluit, adviseer ik u zo spoedig mogelijk bij de NVAO een aanvraag voor de toets nieuwe opleiding in te dienen. Voor de registratie van uw opleiding kunt u gebruik maken van a-Croho. Mocht u vragen hebben over de registratie, dan kunt u contact opnemen met ssg@duo.nl.

Onze referentie
38325432

Een afschrift van deze brief is verzonden aan de CDHO, de NVAO, DUO-Groningen, de Inspectie van het Onderwijs en de UNL.

Met vriendelijke groet,

de minister van Onderwijs, Cultuur en Wetenschap,
namens deze,
de directeur Hoger Onderwijs en Studiefinanciering,



Ministerie van Onderwijs, Cultuur en Wetenschap
T.a.v. de Minister
Dhr. dr. R.H. Dijkgraaf
Postbus 16375
2500 BJ DEN HAAG

Postadres
Postbus 85498
2508 CD Den Haag
Bezoekadres
Parkstraat 83
2514 JG Den Haag
T: 070 8505300
W: www.cdho.nl
E: info@cdho.nl

<i>Onderwerp</i>	<i>Ons Kenmerk</i>	<i>Datum</i>
Nieuwe opleiding Universiteit Leiden Voltijd wo bachelor Cybersecurity & Cybercrime Den Haag	2023/019	17/04/2023

Geachte heer Dijkgraaf,

Op 20/03/2023 heeft de Commissie Doelmatigheid Hoger Onderwijs het voornemen ontvangen van de Universiteit Leiden om de wo bachelor Cybersecurity & Cybercrime als bekostigde opleiding te verzorgen te Den Haag (brief van 20/03/2023 met kenmerk 2023/SAZ/1646727). De aanvraag was voorzien van alle voor de beoordeling benodigde gegevens en is door de commissie in behandeling genomen.

Advies Commissie Doelmatigheid Hoger Onderwijs

Gelet op het hiernavolgende adviseert de commissie u om positief te besluiten op het verzoek van de Universiteit Leiden om de wo bachelor Cybersecurity & Cybercrime als bekostigde opleiding te Den Haag te verzorgen. De commissie adviseert daarbij de toestemming te beperken tot de voltijdvariant op grond van art. 6.2 lid 3 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Beoordelingskader

De wettelijke grondslag voor dit advies is gelegen in art. 6.2 van de WHW. Voorts heeft de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018, verder te noemen de Regeling; voor de commissie als leidraad gediend. Het beoordelingskader treft u in de bijlage bij dit advies aan.

Omschrijving van de aanvraag

De aanvrager wil de opleiding Cybersecurity & Cybercrime in Den Haag vestigen. Het gaat om een Nederlandstalige wo bachelor die de aanvrager in het Croho onderdeel Sectoroverstijgend wil laten registreren. De voorgenomen opleiding omvat 180 studiepunten en de aanvrager wil deze in voltijdvorm aanbieden.

De opleiding is opgezet als een brede bachelor waarin de onderwerpen cybersecurity en cybercrime vanuit vier disciplines worden benaderd, zijnde bestuurskunde, informatica, criminologie en rechten. Elk van de vier disciplines komt ongeveer in gelijke mate aan bod. Verder worden er in de opleiding meerdere vakken aangeboden die gericht zijn op het aanleren van vaardigheden zoals kritisch denkvermogen, ethische reflectie, schrijfvaardigheden en communicatieve vaardigheden.

De opleiding is toegankelijk voor studenten met een vwo-diploma met een Natuur en Gezondheid- of Natuur en Techniekprofiel met interesse in maatschappij, media, cultuur en filosofie of een Economie en Maatschappij- of Cultuur en Maatschappij-profiel met ten minste Wiskunde A of B in het pakket en interesse in toepassingen van digitale technologieën.

Afgestudeerden van de opleiding kunnen na het afronden van een relevante wo masteropleiding onder meer functies als chief information security officer (CISO), cyber incident responder, cyber legal, policy and compliance officer, cybersecurity researcher en digital forensics investigator vervullen.

Motivering

De aanvraag voldoet naar mening van de commissie aan de criteria a en b in art. 4 lid 1 van de Regeling.

Beoordeling criterium a

De aanvrager stelt dat de wo bachelor Cybersecurity & Cybercrime aansluit op een arbeidsmarktbehoefte in combinatie met een maatschappelijke en een wetenschappelijke behoefte.

Beoordeling arbeidsmarktbehoefte

Ter onderbouwing van de arbeidsmarktbehoefte in Nederland beroept de aanvrager zich op de 'Nederlandse Cybersecuritystrategie 2022-2028: Ambities en acties voor een digitaal veilige samenleving' (2022), de agenda 'NCSEA: Nationale Cybersecurity Educatie Agenda' van dcypher (2020), het 'Adviesrapport Integrale Aanpak Cyberweerbaarheid' van de Cyber Security Raad (2021), de prognoses voor opleidingstypen zoals deze zijn opgenomen in ROA's Arbeidsmarktinformatiesysteem (AIS), het rapport 'De arbeidsmarkt naar opleiding en beroep tot 2026' van het ROA (2021), het factsheet 'Update Arbeidsmarktprognoses tot 2026' van het ROA (2021), het rapport 'Studie & Werk 2022: De arbeidsmarktpositie van hbo- en wo-alumni' van SEO Economisch Onderzoek (2022), het rapport 'Duiding arbeidsmarktontwikkelingen' van het UWV (2022), de Spanningsindicator en het Dashboard Vacaturemarkt van het UWV (www.werk.nl/arbeidsmarktinformatie/dashboards), het rapport 'Verwachtingen werkgevers voor 2021' van het UWV (2021), het rapport 'Kansrijke Beroepen' van het UWV (2021), de barometer 'ICT-beroepen: Barometer arbeidsmarkt' van het UWV (2021), het rapport 'Arbeidsmarktonderzoek ICT met topsectoren: Naar een digitaal vaardiger beroepsbevolking' van Berenschot (2019) en de resultaten van een werkveldsessie waar elf vertegenwoordigers van tien potentiële werkgevers bij betrokken zijn geweest (2022).

Verder wordt de internationale arbeidsmarktbehoefte door de aanvrager onderbouwd op basis van het rapport 'Cybersecurity Skills Development in the EU' van de European Union Agency for Cybersecurity (2019), het rapport '(ISC)2 Cybersecurity Workforce Study' van (ISC)2 (2022), het rapport 'Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education' van de European Union Agency for Cybersecurity (2021) en het factsheet 'Cyber Security Skill Gaps and Shortages in the UK Cyber Sector in 2021' van het Department for Digital, Culture, Media & Sport (2021).

De aanvrager stelt bij de onderbouwing van de arbeidsmarktbehoefte voorop dat de arbeidsmarkt rond cybersecurity en cybercrime sterk in beweging is en dat de banen in dit veld onder verschillende sectoren worden ingedeeld (zoals ICT of openbaar bestuur). De aanvrager acht het daarom lastig om de arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding te kwantificeren. Hiertoe verwijst de aanvrager als illustratie naar de 'Nederlandse Cybersecuritystrategie 2022-2028: Ambities en acties voor een digitaal veilige samenleving'

(2022), de agenda 'NCSEA: Nationale Cybersecurity Educatie Agenda' van dcypher (2020) en het 'Adviesrapport Integrale Aanpak Cyberweerbaarheid' van de Cyber Security Raad (2021). De commissie constateert dat de cybersector interdisciplinair van aard is, maar merkt op dat ook bij interdisciplinaire opleidingen een arbeidsmarktbehoefte te kwantificeren is.

De commissie stelt voorop dat, hoewel een wo bacheloropleiding een kwalificatie is om de arbeidsmarkt te betreden, de praktijk over het algemeen is dat afgestudeerde wo bachelors doorstuderen om een mastergraad te behalen. Daarom moet op grond van de Regeling duidelijk worden gemaakt naar welke masteropleiding de afgestudeerde wo bachelors kunnen doorstromen en of er een arbeidsmarktbehoefte is aan deze wo masterafgestudeerden. De aanvrager heeft aangegeven dat afgestudeerden van de voorgenomen opleiding direct toegang hebben tot de volgende wo masters die de aanvrager zelf aanbiedt: Crisis and Security Management, Crime and Criminal Justice (ingeschreven in het Croho als Criminaliteit en Rechtshandhaving), ICT in Business and the Public Sector en Forensische Criminologie. Verder geeft de aanvrager aan dat afgestudeerden van de voorgenomen opleiding onder voorwaarden in een groot aantal andere wo masters kunnen instromen, waaronder Computer Science, Management van de Publieke Sector, Cyber Security, Bestuurskunde, Computing Science en European Law and Global Affairs. De aanvrager geeft aan dat studenten de toegang tot deze opleidingen onder meer door middel van de minorruimte in het derde jaar kunnen verwerven.

De aanvrager beschouwt twee opleidingstypen die zijn opgenomen in ROA's AIS als relevant voor de voorgenomen opleiding Cybersecurity & Cybercrime, zijnde de opleidingstypen bachelor informatica en bachelor recht. De aanvrager beroept zich niet op master opleidingstypen. De commissie kijkt bij wo bacheloropleidingen in eerste instantie naar de master opleidingstypen waar mogelijke vervolgoopleidingen in zijn opgenomen.

De commissie acht het opleidingstype master recht ten dele relevant omdat hierin mogelijke vervolgoopleidingen zoals Forensische Criminologie en Criminaliteit en Rechtshandhaving zijn opgenomen naast een groot aantal zeer specialistische opleidingen in de rechten waar afgestudeerden van de voorgenomen opleiding niet in kunnen stromen. ROA typeert de vooruitzichten in 2026 voor afgestudeerden van dit opleidingstype als goed en verwacht grote knelpunten in de toekomstige personeelsvoorziening (zie Tabel 1).

Tabel 1: Arbeidsmarktprognoses opleidingstype master recht

Opleidingstype	Arbeidsmarktprognose variabele Indicator	Aantal	Gem.		Typering
			Totaal % 6 jr.	jaarlijks %	
> > Master - recht	verwachte uitbreidingsvraag tot 2026	12500	11	1.8	erg hoog
> > Master - recht	verwachte vervangingsvraag tot 2026	17500	16	2.5	gemiddeld
> > Master - recht	verwachte baanopeningen tot 2026	30100	27	4.1	gemiddeld
> > Master - recht	verwachte instroom van schoolverlaters tot 2026	22200	20	3.1	gemiddeld
> > Master - recht	ITKP toekomstige knelpunten personeelsvoorziening in 2026	0.96			groot
> > Master - recht	ITA toekomstige arbeidsmarktsituatie in 2026	0.96			goed

Bron: ROA, AIS

Daarnaast acht de commissie het opleidingstype master informatica ten dele relevant omdat de mogelijke vervolgoopleiding ICT en Business in de Publieke Sector hierin is opgenomen naast een

groot aantal zeer specialistische ICT-opleidingen waar afgestudeerden van de voorgenomen opleiding niet in kunnen stromen. ROA typeert de vooruitzichten in 2026 voor afgestudeerden van dit opleidingstype als goed en verwacht grote knelpunten in de toekomstige personeelsvoorziening (zie Tabel 2).

Tabel 2: Arbeidsmarktprognoses opleidingstype master informatica

Opleidingstype	Arbeidsmarktprognose variabele	Indicator	Aantal	Gem.		Typering
				Totaal	jaarlijks	
> > Master - informatica	verwachte uitbreidingsvraag tot 2026		4100	11	1.7	erg hoog
> > Master - informatica	verwachte vervangingsvraag tot 2026		6500	17	2.6	gemiddeld
> > Master - informatica	verwachte baanopeningen tot 2026		10600	27	4.1	gemiddeld
> > Master - informatica	verwachte instroom van schoolverlaters tot 2026		8500	22	3.3	gemiddeld
> > Master - informatica	ITKP toekomstige knelpunten personeelsvoorziening in 2026	0.95				groot
> > Master - informatica	ITA toekomstige arbeidsmarktsituatie in 2026	0.95				goed

Bron: ROA, AIS

Hoewel de commissie aanneemt dat de meerderheid van de studenten van de voorgenomen opleiding een vervolgopleiding zal volgen, neemt de commissie ook de prognoses voor relevante bacheloropleidingstypen mee in de overweging. De commissie constateert echter dat de door de aanvrager aangehaalde opleidingstypen bachelor recht en bachelor informatica dermate weinig verwante opleidingen bevatten dat zij niet relevant kunnen worden geacht. De interdisciplinaire aard van de opleiding maakt dat deze niet duidelijk in een van de huidige bachelor opleidingstypen van het ROA past.

De commissie concludeert dat de prognoses die zijn opgenomen in ROA's AIS voor de opleidingstypen die ten dele relevant zijn voor de onderhavige opleiding een positief beeld geven van de arbeidsmarktperspectieven voor afgestudeerden van de voorgenomen opleiding Cybersecurity & Cybercrime.

De aanvrager verwijst ook naar het rapport 'De arbeidsmarkt naar opleiding en beroep tot 2026' van het ROA (2021, p. 28), waar de verwachte knelpunten voor beroepsklassen worden besproken. De aanvrager stelt dat afgestudeerden van de voorgenomen opleiding in de volgende beroepsklassen terecht kunnen komen: openbaar bestuur, veiligheid en juridische beroepen, ICT-beroepen en managers. De commissie is van mening dat de beroepsklassen zoals deze zijn opgenomen in het rapport (en tevens in het AIS) te veel niet en nauwelijks relevante beroepsgroepen bevatten en daardoor geen representatief beeld geven van de specifieke arbeidsmarkt waar afgestudeerden van de voorgenomen opleiding werkzaam zullen zijn. Om deze reden laat de commissie de prognoses voor beroepsklassen buiten beschouwing.

Verder haalt de aanvrager het factsheet 'Update Arbeidsmarktprognoses tot 2026' van het ROA (2021) aan, waarin wordt aangegeven dat er in het algemeen tot 2026 meer dan 2,3 miljoen baanopeningen worden verwacht tegenover een algemene instroom van 1,6 miljoen afgestudeerden. De beste baankansen bevinden zich volgens dit factsheet in de techniek, de zorg en het onderwijs. De aanvrager refereert ook aan het rapport 'Duiding arbeidsmarktontwikkelingen' van het UWV (2022, p. 2) om te stellen dat er in het algemeen sprake is van een krappe arbeidsmarkt waarin het moeilijk is om personeel te vinden. Daarnaast

stelt de aanvrager op grond van het rapport 'Studie & Werk 2022: De arbeidsmarktpositie van hbo- en wo-alumni' van SEO Economisch Onderzoek (2022, p. i, 7) vast dat de baankansen van afgestudeerden in het wetenschappelijk onderwijs in het algemeen hoog zijn en een stijgende lijn vertonen. De commissie constateert dat deze bronnen inderdaad blijken te geven van een krappe arbeidsmarkt en goede baankansen voor wo-afgestudeerden, maar dat deze bronnen te algemeen zijn om blijken te kunnen geven van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De aanvrager verwijst vervolgens naar de gegevens afkomstig uit de Spanningsindicator en het Dashboard Vacaturemarkt van het UWV (www.werk.nl) betreffende de voornoemde beroepsklassen openbaar bestuur, veiligheid en juridische beroepen, ICT-beroepen en managers op zowel een landelijke als regionale schaal (regio Haaglanden). De commissie merkt op dat de arbeidsmarkt begin 2020 is gekrompen als gevolg van de coronacrisis en dat deze krimp vervolgens is omgeslagen naar een (zeer) grote krapte op de arbeidsmarkt die zichtbaar is bij alle beroepsgroepen en alle sectoren. Het feit dat de arbeidsmarktspanning bij de door de aanvrager relevant geachte beroepsklassen als (zeer) krap wordt getypeerd en het aantal vacatures daarbinnen is toegenomen, is daarom niet onderscheidend. De commissie kent daarom minder gewicht toe aan deze bronnen en stelt vast dat zij een (zeer) kleine positieve indicatie geven van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Op grond van het rapport 'Verwachtingen werkgevers voor 2021' van het UWV (2021, p. 4, 6) stelt de aanvrager dat werkgevers de komende jaren een tekort aan hoogopgeleid ICT-personeel verwachten. Werkgevers bij de overheid geven ook aan groei te verwachten en noemen daarbij ICT als specifieke beroepsgroep waar tekorten bestaan. De commissie constateert dat de voorgenomen opleiding de mogelijkheid biedt om een vervolgopleiding in de ICT te volgen en dat deze bron als zodanig een positieve indicatie geeft van de arbeidsmarktkansen van afgestudeerden die een dergelijke vervolgopleiding kiezen.

Het rapport 'Kansrijke Beroepen' van het UWV (2021) vermeldt volgens de aanvrager dat afgestudeerden onder meer in aanmerking kunnen komen voor hierin als kansrijk aangemerkte beroepen zoals 'beleidsmedewerker bestuurlijk-juridisch' en 'jurist/juridisch adviseur' alsmede verschillende functies binnen de ICT-beroepen (alle op hoger/wetenschappelijk beroepsniveau). De commissie constateert dat in de meest recente editie van dit rapport (2022, p. 9-10) de twee genoemde beroepen nog steeds als kansrijk zijn aangemerkt (de eerstgenoemde nu als 'beleidsadviseur bestuurlijk-juridisch') en dat er ook onder de ICT-beroepen onder meer beroepen zoals 'Securityspecialisten ICT' zijn opgenomen waar afgestudeerden van de voorgenomen opleiding (na het volgen van een relevante vervolgopleiding) voor in aanmerking zouden kunnen komen. De aanvrager verwijst tevens naar de barometer 'ICT-beroepen: Barometer arbeidsmarkt' van het UWV (2021), waar security specialisten ook als een van de 'meest kansrijke ICT-beroepen' wordt genoemd. De commissie constateert dat deze bronnen een positieve indicatie geven van de arbeidsmarktkansen van afgestudeerden van de voorgenomen opleiding.

Verder verwijst de aanvrager naar de voornoemde 'Nederlandse Cybersecuritystrategie 2022-2028: Ambities en acties voor een digitaal veilige samenleving' (2022, p. 42), waarin wordt gesteld dat er meer opleidingsplekken nodig zijn op mbo-, hbo- en wo-niveau die aansluiten op de (cybersecurity-)arbeidsmarkt. Ook het rapport 'Arbeidsmarktonderzoek ICT met topsectoren: Naar een digitaal vaardiger beroepsbevolking' van Berenschot (2019, p. 8, 69) wordt aangehaald, waarin wordt gesteld dat er binnen de ICT-sector een groeiend arbeidskrachtentekort bestaat en dat de instroom in het onderwijs niet toereikend is om dit tekort op te lossen. Ook wordt er in deze bron gesteld dat inzet op digitale technologie noodzakelijk is om Nederland concurrerend te houden. Hierbij wordt onder andere cybersecurity genoemd als een belangrijke sector waar in kan worden geïnvesteerd. De commissie constateert dat deze bronnen blijken te geven van een behoefte aan meer afgestudeerden in de ICT-sector in het algemeen en in de cybersecurity-sector in het bijzonder.

De aanvrager gaat in het dossier ook in op de regionale arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding. Hierbij noemt de aanvrager verschillende organisaties die in de regio Den Haag zijn gevestigd (zoals diverse ministeries, de AIVD en diverse telecombedrijven) die volgens de aanvrager behoefte hebben aan afgestudeerden van de voorgenomen opleiding. De aanvrager onderbouwt deze aanname niet, maar de commissie acht het aannemelijk dat genoemde organisaties een zekere behoefte hebben aan medewerkers met kennis van cyberveiligheid. Hier blijkt echter geen concrete arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding uit.

De aanvrager verwijst in de inleiding van het dossier verder naar de resultaten van een werkveldsessie waar elf vertegenwoordigers van tien potentiële (overwegend regionale) werkgevers bij betrokken zijn geweest (2022). De aanvrager vermeldt de namen en functies van de respondenten en de bedrijven waar zij werkzaam zijn. De commissie constateert dat de respondenten in een positie zijn om relevante uitspraken te kunnen doen wat betreft de arbeidsmarktbehoefte.

De aanvrager vermeldt dat de respondenten onderschrijven dat er een tekort bestaat aan hooggekwalificeerd personeel op het gebied van cybersecurity en cybercrime en dat dit tekort naar hun verwachting zal oplopen. De respondenten geven ook aan te denken dat de multidisciplinaire aard van de opleiding voorziet in een grote behoefte omdat de meeste kennis in de cybersecurity nu te veel monodisciplinair is belegd. De commissie constateert dat de benoemde resultaten blijken te geven van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Ter onderbouwing van de internationale arbeidsmarktbehoefte verwijst de aanvrager naar het rapport 'Cybersecurity Skills Development in the EU' van de European Union Agency for Cybersecurity (2019, p. 8-11), waarin wordt gesteld dat het tekort aan arbeidskrachten in cybersecurity en cybercrime op internationale schaal al groot is en dat er wordt verwacht dat dit tekort in de komende jaren zal oplopen. Het rapport geeft onder meer aan dat de geschatte tekorten in Europa tussen 2018 en 2019 zijn opgelopen van 142.000 naar 291.000 gezochte medewerkers (zonder niveau aanduiding). Het rapport '(ISC)2 Cybersecurity Workforce Study' van (ISC)2 (2022, p. 7) stelt dat de tekorten in Europa in 2022 waren opgelopen tot ongeveer 317.000 gezochte medewerkers (zonder niveau aanduiding). In het door de aanvrager aangehaalde rapport 'Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education' van de European Union Agency for Cybersecurity (2021) wordt beargumenteerd dat deze tekorten vooral door middel van meer hoger onderwijs in de richting van cybersecurity moeten worden opgelost. De aanvrager stelt dat de voorgenomen opleiding op dit plan aansluit. De commissie volgt de aanvrager in deze stelling en constateert dat deze bronnen een internationale arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding aannemelijk maken.

De commissie merkt ten slotte op dat de aanvrager refereert aan het factsheet 'Cyber Security Skill Gaps and Shortages in the UK Cyber Sector in 2021' van het Department for Digital, Culture, Media & Sport (2021) om aan te geven dat er in het Verenigd Koninkrijk 'skill gaps' worden opgemerkt bij werknemers en werkzoekenden binnen cyber-gerelateerde functies. Dit factsheet noemt vaardigheden op zowel technologisch gebied als op het gebied van rechten, bedrijfskunde en 'soft skills'. De aanvrager beargumenteert dat deze patronen ook zichtbaar zijn op de Nederlandse arbeidsmarkt en stelt dat de voorgenomen opleiding beoogt aandacht te besteden aan deze verschillende vaardigheden. De commissie acht het op grond van het bovenstaande aannemelijk dat deze vaardigheden ook op de Nederlandse arbeidsmarkt worden gezocht en volgt de aanvrager in de stelling dat de voorgenomen opleiding hier aandacht aan besteedt. De commissie constateert dat deze bron een kwalitatieve arbeidsmarktbehoefte aannemelijk maakt.

De commissie concludeert op grond van het bovenstaande dat de aanvrager aannemelijk heeft gemaakt dat er een arbeidsmarktbehoefte bestaat aan de voorgenomen opleiding Cybersecurity & Cybercrime.

Beoordeling maatschappelijke behoefte

De aanvrager onderbouwt de maatschappelijke behoefte aan de hand van de volgende bronnen: het 'Cybersecuritybeeld Nederland' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022), de 'Nederlandse Digitaliseringsstrategie 2021' (2021) en het rapport 'Wat de toenemende cyberdreiging van IT-dienstverleners vraagt' van ING Research (2022).

De aanvrager beargumenteert dat het gebruik van genetwerkte digitale technologieën in onze samenleving gemeengoed is geworden en dat zij de ruggengraat vormen van de samenleving. Op basis van het 'Cybersecuritybeeld Nederland' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022, p. 7-8) stelt de aanvrager dat dit naast voordelen ook risico's omvat, zoals een kans op maatschappelijke ontwrichting bij het uitvallen van deze technologieën (bijvoorbeeld door cyberaanvallen). Dit maakt volgens de aanvrager dat cybersecurity één van de meest urgente thema's is geworden in de moderne samenleving. De aanvrager verwijst naar de 'Nederlandse Digitaliseringsstrategie 2021' (2021, p. 12) die vermeldt dat 36% van de economische groei in Nederland voortkomt uit digitalisering, maar stelt ook onder verwijzing naar het rapport 'Wat de toenemende cyberdreiging van IT-dienstverleners vraagt' van ING Research (2022, p. 7) dat de economische schade als gevolg van cybercrime momenteel op 8 tot 12 miljard euro per jaar wordt geschat. De aanvrager stelt dat de voortschrijdende digitalisering de urgentie van digitale veiligheid blijft vergroten en dat hiervoor veel kennis en kunde nodig is. De aanvrager stelt dat de voorgenomen opleiding hierop aansluit. De commissie volgt de aanvrager in deze stelling en concludeert dat dit blijk geeft van een maatschappelijke behoefte aan afgestudeerden van de voorgenomen opleiding.

De commissie concludeert dat de aanvrager heeft aangetoond dat er een maatschappelijke behoefte bestaat aan de voorgenomen opleiding Cybersecurity & Cybercrime.

Beoordeling wetenschappelijke behoefte

De aanvrager onderbouwt de wetenschappelijke behoefte aan de hand van de volgende bronnen: de onderzoeksagenda 'NCSRA III: National Cyber Security Research Agenda' van dcypher (2018), de website van het NWO (www.nwo.nl/onderzoeksprogrammas/nationale-wetenschapsagenda/thematische-programmering/cybersecurity) en de 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig' (2015).

De aanvrager beargumenteert onder de wetenschappelijke behoefte dat cybersecurity oorspronkelijk vooral werd gezien als een technische uitdaging, maar dat er tegenwoordig ook meer aandacht wordt besteed aan de economische, juridische en bestuurlijke uitdagingen die hieraan gekoppeld zijn. Als gevolg hiervan wordt er ook onderzoek gedaan naar cybersecurity door sociaal wetenschappers zoals bestuurskundigen en criminologen. Dit blijkt volgens de aanvrager onder meer uit de onderzoeksagenda 'NCSRA III: National Cyber Security Research Agenda' van dcypher (2018, e.g. p. 35), waarin de pijlers voor cybersecurity-onderzoek worden besproken. Bij elke pijler wordt aangegeven welke verbanden bestaan tussen de alfa-, bèta- en gammawetenschappen. Verder geeft de aanvrager op basis van de website van het NWO (www.nwo.nl) dat cybersecurity één van de 27 thema's is binnen de Nationale Wetenschapsagenda (zijnde het thema 'Cybersecurity - naar een veilig en betrouwbaar digitaal domein') en dat in 2021 vijf multidisciplinaire onderzoeksprojecten zijn gestart binnen dit thema. Ten slotte verwijst de aanvrager ook naar de 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig' (2018, p. 39), waarin ook wordt aangegeven dat kennisontwikkeling op het gebied van cybersecurity interdisciplinair onderzoek omvat.

De aanvrager stelt dat afgestudeerden van de voorgenomen opleiding met hun multidisciplinaire blik (en na het volgen van een toepasselijke vervolgopleiding) in de toekomst een waardevolle bijdrage kunnen leveren aan wetenschappelijk onderzoek op het gebied van cybersecurity en cybercrime door middel van onder meer promotietrajecten. De commissie acht deze stelling plausibel en concludeert op grond hiervan dat de aanvrager heeft aangetoond dat er een wetenschappelijke behoefte bestaat aan afgestudeerden van de voorgenomen opleiding.

De commissie concludeert dat de aanvrager heeft aangetoond dat er een wetenschappelijke

behoefte bestaat aan de voorgenomen opleiding Cybersecurity & Cybercrime.

De commissie concludeert dat de aanvraag aansluit op een maatschappelijke, een wetenschappelijke en een arbeidsmarktbehoefte. De aanvraag voldoet aan criterium a in art. 4 lid 1 van de Regeling.

Beoordeling criterium b

Vanaf 20/03/2023 is op de website van de CDHO kennisgegeven van het voornemen van de Universiteit Leiden om de wo bachelor Cybersecurity & Cybercrime in Den Haag aan te bieden. Hiermee is aan de instellingen voor hoger onderwijs de mogelijkheid gegeven om hun zienswijzen op dit voornemen kenbaar te maken. Er zijn geen zienswijzen ingediend.

De commissie stelt op basis van de afbakening die de aanvrager heeft aangeleverd vast wat het verwante aanbod van de aangevraagde opleiding is. Verwante opleidingen komen inhoudelijk sterk overeen en leiden op tot (min of meer) dezelfde beroepen (uitstroomprofiel(en)). Bij de inhoud wordt gekeken of de kennisgebieden en vaardigheden die in het curriculum van de voorgenomen opleiding zijn opgenomen overlap vertonen met de bestaande opleidingen. Verder worden de instroomdoelgroep en de onderwijsvariant (voltijd, deeltijd of duaal) meegewogen bij de afbakening.

De aanvrager is van mening dat er geen sterk verwante opleidingen zijn. De aanvrager acht de wo bachelor Computing Science van de Radboud Universiteit Nijmegen aanverwant aan de voorgenomen opleiding vanwege de daarin opgenomen specialisatie Cyber Security. De aanvrager noemt verder meerdere hbo bachelors, wo masters en één hbo master als aanverwant aanbod. Daarnaast is de aanvrager van mening dat de volgende wo bacheloropleidingen die zij zelf aanbiedt "raakvlakken" hebben met de voorgenomen opleiding: Bestuurskunde (ook aangeboden door Erasmus Universiteit Rotterdam, Technische Universiteit Delft, Radboud Universiteit Nijmegen en Tilburg University), Criminologie (ook aangeboden door Erasmus Universiteit Rotterdam en Vrije Universiteit Amsterdam), International Studies, Informatica (ook aangeboden door Rijksuniversiteit Groningen, Universiteit Utrecht, Universiteit van Amsterdam en Open Universiteit), Data Science and Artificial Intelligence (nog niet gestart, al aangeboden door Universiteit Maastricht), Rechtsgeleerdheid (ook aangeboden door acht andere instellingen), Security Studies en Urban Studies.

De aanvrager gebruikt in het dossier de termen "aanverwant" en "vertoont raakvlakken". Deze worden door de commissie beide begrepen als vergelijkbaar met de door de commissie gebruikte term "aanverwant".

De commissie volgt de aanvrager in de constatering dat er tot op heden geen sterk verwante opleidingen worden aangeboden. De commissie is verder van mening dat de volgende door de aanvrager genoemde opleidingen aanverwant zijn aan de voorgenomen opleiding: Security Studies, Bestuurskunde, Computing Science, Criminologie en Informatica. De instroom van de aanverwante opleidingen is in de afgelopen vijf jaar gestegen (zie Tabel 3).

De commissie stelt vast dat binnen de systematiek van de Regeling hbo bachelors, hbo masters en wo masters niet verwant worden geacht aan wo bachelors omdat zij een ander niveau en een andere oriëntatie hebben. De door de aanvrager genoemde opleidingen op deze niveaus en oriëntaties worden daarom door de commissie niet meegenomen in de onderstaande overweging. De commissie is verder van mening dat de volgende wo bacheloropleidingen die door de aanvrager zijn aangedragen nauwelijks verwantschap tonen met de voorgenomen opleiding: International Studies, Data Science and Artificial Intelligence, Rechtsgeleerdheid en Urban Studies. De commissie acht deze opleidingen nauwelijks verwant omdat zij een substantieel ander programma aanbieden dan de voorgenomen opleiding, hun studenten voor andere beroepen opleiden, en/of een andere instroomgroep bedienen.

Tabel 3: Instroom eerstejaarsstudenten in verwant voltijd bekostigd onderwijsaanbod

Opleiding	Instelling	'17-'18		'18-'19		'19-'20		'20-'21		'21-'22	
		VT	DT	VT	DT	VT	DT	VT	DT	VT	DT
B Security Studies (59320)	Universiteit Leiden (21PB), 's-Gravenhage	122		210		249		293		264	
	Erasmus Universiteit Rotterdam (21PE), Rotterdam	301		350		384		421		450	
B Bestuurskunde (56627)	Radboud Universiteit Nijmegen (21PM), Nijmegen	149		161		134		111		116	
	Tilburg University (21PN), Tilburg	82		115		119		84		57	
B Computing Science (59326)	Universiteit Leiden (21PB), 's-Gravenhage	326		342		332		344		397	
	Radboud Universiteit Nijmegen (21PM), Nijmegen			178		193		172		163	
B Criminologie (56469)	Erasmus Universiteit Rotterdam (21PE), Rotterdam	123		126		126		132		130	
	Universiteit Leiden (21PB), Leiden	158	4	158	5	158	5	157	4	152	4
B Informatica (56978)	Vrije Universiteit Amsterdam (21PL), Amsterdam	125		126		126		129		128	
	Rijksuniversiteit Groningen (21PC), Groningen	117		109		192		164		123	
B Informatica (56978)	Universiteit Leiden (21PB), 's-Gravenhage	31		36		34		18			
	Universiteit Leiden (21PB), Leiden	124	1	127	1	197	3	196		250	
	Universiteit Utrecht (21PD), Utrecht	186		222		231		252		231	
	Universiteit van Amsterdam (21PK), Amsterdam	106		130		148		120		151	
Totaal Instroom		1950	5	2390	6	2623	8	2593	4	2612	4

Bron: DUO

De aanvrager heeft een prognose gemaakt van de instroom in de voorgenomen opleiding op grond van een instroomanalyse die is uitgevoerd door het NIDAP in opdracht van de aanvrager. De aanvrager verwacht dat er bij de start van de opleiding tussen de 165 en 372 studenten zullen instromen en dat de instroom in 2035 tussen de 242 en 549 zal liggen. De commissie acht deze prognose hoog gezien de instroom in het verwante aanbod.

Als de instroom in de bestaande opleidingen en de verwachte instroom in de voorgenomen wo bachelor Cybersecurity & Cybercrime wordt afgezet tegen de arbeidsmarktbehoefte die bij criterium a aannemelijk is gemaakt en de maatschappelijke en wetenschappelijke behoefte die daar zijn aangetoond, blijkt dat er voldoende ruimte is om deze opleiding binnen het bekostigde domein vorm te geven.

Vestiging van de opleiding in Den Haag heeft mogelijk enig negatief effect op de landelijke spreiding van het onderwijsaanbod omdat de aanverwante wo bachelor Security Studies van de aanvrager hier ook is gevestigd. De commissie is echter van mening dat de voorgenomen opleiding geen onevenredig negatief effect zal hebben op de instroom van deze opleiding omdat deze instroom substantieel genoeg is om enige krimp op te kunnen vangen.

De commissie concludeert dat er voldoende ruimte in het landelijk aanbod bestaat om de wo bachelor Cybersecurity & Cybercrime te realiseren. De aanvraag voldoet aan criterium b in art. 4 lid 1 van de Regeling.

Gelet op het vorenstaande adviseert de Commissie Doelmatigheid Hoger Onderwijs u om positief te besluiten op het voorliggende verzoek. De commissie adviseert daarbij de toestemming te beperken tot de voltijdvariant op grond van de bevoegdheid in art. 6.2 lid 3 WHW.

Advies aan de NVAO over de naamkeuze en Croho indeling

De commissie heeft geconstateerd dat de voorgenomen opleiding dermate afwijkt van het bestaande verwante opleidingsaanbod, dat dit de keuze voor een andere naam rechtvaardigt.

Daarnaast heeft de commissie geconstateerd dat de aanvrager de wo bachelor Cybersecurity & Cybercrime in het Croho onderdeel Sectoroverstijgend wil indelen. Dit voorstel sluit aan op het interdisciplinaire karakter van de opleiding.

De NVAO ontvangt dit advies, zodat zij dit kan opnemen in het informatiedossier voor het panel ten behoeve van de toets nieuwe opleiding.

De Commissie Doelmatigheid Hoger Onderwijs



drs. P.M.M. Rullmann

Voorzitter CDHO

Bijlage:

Beoordelingskader macrodoelmatigheid nieuwe opleiding of nevenvestiging

Aan de hand van de in de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018 genoemde voorwaarden worden voornemens tot het verzorgen van een nieuwe opleiding beoordeeld op doelmatigheid. Een nieuwe opleiding kan volgens artikel 4 van deze Regeling alleen doelmatig worden geacht indien het voornemen voldoet aan de criteria a en b.

Volgens criterium a heeft het instellingsbestuur aangetoond dat er behoefte bestaat aan de nieuwe opleiding of nevenvestiging, zijnde overwegend een arbeidsmarktbehoefte, dan wel een overwegend maatschappelijke behoefte in combinatie met een arbeidsmarktbehoefte, dan wel een overwegend wetenschappelijke behoefte in combinatie met een arbeidsmarktbehoefte.

Volgens criterium b dient het instellingsbestuur aan te tonen dat in de behoefte die bij criterium a is aangetoond niet door het bestaande opleidingsaanbod wordt voorzien.

Advies aan de NVAO over naamkeuze en Croho indeling

In de Toelichting op de Regeling is aangegeven dat de CDHO ook een rol heeft bij de beoordeling van de voorgestelde naam en voertaal van de opleiding en bij de voorgestelde positionering in het Croho.

Wat betreft de opleidingsnaam: de CDHO kijkt of de voorgestelde naam van de opleiding passend is, gelet op de namen van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen dezelfde naam krijgen, om de transparantie van het opleidingsaanbod voor studiekeizers en werkgevers te borgen. In het Croho kan ook een internationale (Engelse) naam worden geregistreerd. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de naamkeuze gerechtvaardigd is gelet op de inhoud van de opleiding en de namen van vergelijkbare opleidingen (artikel 5.7, vierde lid, onderdeel a, van de WHW).

Wat betreft de positie in het Croho: de CDHO kijkt of de voorgestelde indeling in het Croho passend is, gelet op de indeling van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen in hetzelfde Croho onderdeel worden geregistreerd, om de transparantie van het opleidingsaanbod voor studiekeizers en werkgevers te borgen. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de voorgestelde indeling in het Croho aansluit bij de ordening van verwante opleidingen.